Risk Management functions in Banks and How Forensic Accountants Can Add Competitive Advantage

Research Project for Emerging Issues / Advanced Topics Course

Masters in Investigative and Forensic Accounting Program

University of Toronto

Prepared by: Kehinde Akere-Azeez

June 18th, 2021

For Prof. Leonard Brooks

Acknowledgements

I appreciate and acknowledge the unfailing patience, support, and assistance that I've received from MFAcc program lecturers and staffs especially, Debby Keown- program officer and many others. I appreciate Ann-Marie Deboran and Richard Lederman my mentors, for their pearls of wisdom and insights towards the successful completion of this project.

I'm most grateful to my wife (Michelle) and children (Abayomi & Bolutife) for their emotional support during my journey into this higher education. I recognize my twin brother (Tai), who has been my source of inspiration and my late mother.

[Most importantly to God Almighty Allah for a successful completion]

Table of Contents

Introduction

This paper examines risk management functions within Canadian Banks and what roles a Forensic Accountant can play to add competitive advantage or value compared to other professionals- traditional financial auditor and risk officer. This will broadly focus on areas such as Enterprise Risk Management (ERM), Anti-Money Laundry (AML), Investigations, Internal Audit (IA), and Compliance. The qualities, academic qualifications, and characteristics that distinguish forensic accountants amongst other professionals when it comes to risk management function was also examined and enumerated. Various legal matters, legislations, and standards that have also emerged as a result of increase demand in the service of a forensic accountant to mitigate risk within financial institutions that stemmed from recent financial scandals and economics meltdown of 2008 and 2009 worldwide were also looked into. In today's super-competitive business environment, culture, strategy and value creation is one ecosystem. Risk management experts, forensic accountants therefore, are expected to respond with speed and agility in identifying risks, risk appetite and designing the remediation techniques to preserve an entity's value-creation activities.

This paper begins by providing history of risk and risk management, followed by organizational risk management governance, risk management process in the banks with specific reference to the hazards that are fundamental to the financial sector at large. A taxonomy of such risks are broken into seven generic types as described by the available works of literature as credit, operational, liquidity, market and systemic, interest rate, regulatory/legal, and counterpart risks.

Canadian banks, just like any other banks, have always faced with credit risk, market risk, liquidity risk, and operational risks among host of others. However, the second COSO 2013 principle enterprise risk management (ERM) is a core focus that targets the top risks and weaknesses of the organization and determines how to balance their strategic opportunities with risk discipline. The COBIT 2019 Core Model contains specific risk governance and management objectives and includes supporting process such as EDM03-Ensured Risk Optimization, APO12-Management Risk (which develops a substantiated view of actual I &T risk in support of risk decisions, measure with critical metrics and specific organizational structures, skills, culture

aspects etc. The new COBIT 2019 approach to Risk Management is expected to confront several weaknesses highlighted in COBIT 5, such as the fragmented manner in which Risk Management has been organized in the past, the historical lack of senior management involvement in the conflict between risk management and performance, the inconsistency used in identifying risk and risk assessment as a result of unclear taxonomies and vaguely defined risk appetite.

With the involvement of a forensic accountant, banks can easily identify and uncover any potential risks, assess and understand possible risk of Money Laundering/Terrorist Financing (ML/TF) and adopt appropriate reactive preventive risk-based measures to mitigate those identified and evaluated risks. Procedures may include, but not limited to, account reconstruction, preparation of source and use of funds, asset tracing, and net worth analyses to reflect evolving ML/TF trends. Forensic accountants can also help to adopt and apply a risk-based approach and framework to ensure that measures to prevent and/or mitigate ML/TF are commensurate with identified risks and aligned with Financial Action Task Force FATF AML/TF framework as amended.

This paper sheds light on the importance of the forensic accountant's skills of business operations understanding and an in-depth knowledge of what could possibly go wrong at any time, how they would affect the business bottom-line and reputations, and actions to take to avoid either the risk or its consequences when risks eventually occur. It is evident that to assess and predict risk accurately, one must possess analytical skills, but from a forensic accountant's point of view, it goes further than that. This assumption can said to be logically founded because a forensic accountant expert will give a dissertation or exposition of scientific or other principles relevant to the circumstances. Barriers to Effective Risk Management are not a new concept, and it continues to gather attention with the revelation and evolution of each new corporate scandal and market crisis. This could stem from different factors or reasons external and internal to Canadian financial institutions such as the willingness to take on higher risks, introduction of e-banking, extending credit facilities to low-income earners and failure to regularly or objectively and fairly report risks to the Board and the senior management.

Several factors have been adduced to explain the developments prejudicial to effective enterprise risk management, such as inability to properly communicate risks to senior management, failure to regularly, objectively, and fairly report or present risks to the Board or senior management by

other risk practitioners in a clearer and more detailed manner like a forensic accountant. Furtherance to the aforementioned points, use of improper risk metrics which induces inaccurate measurements by non forensic accountant experts could be proved elusive and unadoptable for purposes of satisfactory judicial administration. The paper further considers the relevance of a mature risk management approach and the need for establishing responsibility through policies and procedures for reporting on risk, culture and performance, building procedures for the timely escalations. In addition, building a common risk language, shared definitions, a shared culture of risk awareness and clearly understood procedures for measuring, monitoring and dealing with risks are also touched upon in this section.

Forensic accountants/investigators leverage their diversified skills and expertise to provide investigative, auditing, and risk assessment to preserve and stabilize financial and accounting information and integrity. Forensic accountant expertise in big data analytics, data mining etc. can help in an investigation process to analyze electronically stored financial and accounting data. The final application of forensic data analysis is in the inquiry itself, which is also within the domain and expertise of the forensic accountant. Owing to proliferation of electronic data, it has become increasingly crucial for forensic accountant to determine, before any investigation, what relevant information exist and in what format; what security measures in place to protect the data; and what is the organization's standard policies and procedures on record retention and destruction. Review of supporting documents, a judgmental call to testing for the authenticity of the record or of individual signatures on documents that generally involve a highly specialized skill that ultimately possessed by a forensic accountant. With constant revolving and trends in technology and customer expectations, risk management functions have continued to evolve and update over the years across financial institutions and large corporations with global initiatives, customer demands, changes in regulations and the fines levied for non-compliance of these regimes.

This research project investigates how the active involvement of forensic accountants adds value to risk management functions at banks, based on their knowledge of financial processes, data analysis, the study of failed businesses, training on legal processes, investigative matters, loss quantification, and the Standard Practices for Investigative and Forensic Accounting Engagements (SPIFA). The forensic accountant’s background is a game changer in recognizing

the broad risks than occur due to global economic conditions, disruptive technologies, changing consumer demands, financial crimes, and the entity's internal culture which drives strategy and profitability. Accountants, auditors, and risk managers are organizationally placed and perform conceptually different roles, which provide an opportunity for the forensic accountant to help.

Forensic accountants who are involved in enterprise risk management functions, draw from their financial skills, understanding of fraudulent financial transactions, astute acumen of the elements of fraud, and have an awareness of the accumulation of questionable decisions that cascade into business failures. They are looking for the needle in the haystack, telling the story around evidence, researching statutes, standards, and rules, all of which distinguishes them from the traditional auditors, accountants and risk managers. As financial institutions increase in size and offer new products, grow organically or through mergers, business complexity increases, and the skills and technical knowledge of forensic accountants are needed to support regulatory, risk and legislative demands and expectations.

SECTION 1

OVERVIEW OF RISK MANAGEMENT PROCESSES AT BANKS

Efficient and effective risk management is a central focus of financial regulators and financial institutions. Risk management has long been associated with the possibility of accidents (Harrington and Nichaus, 2003, p.7)[1]. As Dionne (2013) observes, new forms of pure risk management emerged in the mid-1950s as an alternative to market insurance when different insurance coverage became very costly and incomplete. In 1997 the Basel Committee on Banking Supervision (BCBS) published its "core principles" and updated them in 2011 to emphasize that bank needed resources to manage systemic risk at the micro prudential level to increase focus on crisis management, recovery measures to reduce the likelihood and impact of failure.

[1] The National Alliance Research Academy-Risk Management Essentials

"Tursoy (2018) proposes that the focus of risk management is to manage the entity's exposure to losses or risks and to protect the value of its assets, and concludes that effective risk management is crucial to financial institutions as they are faced with increasing exposures to risk." A well-designed risk management framework and assessment will allow banks to address emerging risks at an early stage and develop appropriate strategies to control and mitigate those risks before any adverse effects can occur in the bank's operations. Taxonomy of such risks can be broken into seven generic types as described by the available works of literature such as credit risk, liquidity risk, operational risk, market and systematic risks, interest rate risk, regulatory/legal risk and counterparty risk. This summary is wide ranging and perhaps a standardized global definition of macro and micro risk terminology is required in the field. If these threats are clearly defined, they can be managed through diversification and risk mitigation.

1.1 Risk Management at the Board level

The board and senior management members are crucial to creating a dynamic risk culture for risk management practices. By creating a vibrant risk culture, the board must commit to an ongoing process that modifies risks, program designs, implementation systems, and evaluation techniques according to COSO 2017 and other related regulations and standards.

This framework accepts that the board and senior management has an active role in overseeing and monitoring the bank's risk management structure. On the one hand by requiring the management to propose an appropriate and efficient risk management policy, including the development of a "Risk Appetite Framework" allowing for the identification of risks both on a firm-wide basis and per business line. And on the other, by the introduction of the supporting IT systems that will enable top management and the board to gain timely and comprehensive insight in the risk apprehension on an evaluative basis, for each of the business lines and allowing for corrections where due[2].

1.2 Risk Management Framework

Effective risk management can be considered as a fundamental principle of sound governance. A consistent and solid risk culture underlies sound decision-making, outcomes, and accountability. When ERM is adopted and integrated by banks, risk information provides insights into transparency over operations and disruptive and emerging risks. Risk management frameworks

[2] Financial Law Institute-Working Paper Series- WP 2012-04 (WYMEERSCH, E. 2012, p. 2)

(RMF) adopting the International Organization for Standardization 31000:2018 principles, addresses how banks can embed the management of risk into its culture and practices to support the board of directors and senior executives and Chief Information Officers in making informed decisions and provide assurance that a robust risk management approach is adopted across the banking sector.

There are 5 principles which list its key takeaways as the advice given to top management and boards, as follows:

1. Executive Buy-In, which reinforces that executives should provide strong leadership and commitment to the risk management process, ensure it is integrated it across all levels of the corporation and aligned with objectives, strategy and culture of the organization.
2. Considering risks in business decisions, which advises that the boards' roles is to ensure that risks are given full consideration when strategic decisions are being made, as those risks will impact the entity's ability to deliver value.
3. Emphasize Proper Implementation, which states that the board has the responsibility to ensure the ERM process is implemented and that the controls are understood. In the case where the board may not have the expertise to appreciate the significance and impact of certain risks such as cyber, a third-party risk management expert should be retained to provide the relevant context and ensure that the guidelines cover the strategic importance of the cyber domain.
4. Risk Management Is Not One-Size-Fits-All, emphasizes that risk management is an iterative, cyclical actions to customize update risks for relevancy. This ISO document recommends that top leadership to customize its risk profile, culture and risk appetite for the financial institution.
5. Reactivity, which is the fifth principle, makes a recommendation to the board and senior management to a proactive mindset on risk ensuring that risk management flows through all levels and aspects of decision-making of the organization. This includes business continuity, compliance, crisis management, HR, IT and organizational resilience which also commits to the culture, the strategy and values. (Appendix Figure 3: ISO 310000 2018 Value Creation and Protection Principles).

To give a brief overview of the Risk Management Life Cycle, the general concepts and cyclical process of IT and risk management are Risk Identification, Risk Assessment and measurement, Risk response and mitigation, Risk and control monitoring and reporting and the cycle continues to recognize relevant and impactful risks. (Appendix Figure 2: ISACA Depicts the cyclical risk management process (RMLC))

Risk Identification

The first step in identifying the risks a company faces is to define the risk universe (i.e., a list of all possible risks), which includes determining risk appetite and framework. Examples include IT risk, operational risk, regulatory risk, political risk, strategic risk, and credit risk.

After listing all possible risks, the company can then select the risks to which it is exposed and categorize them into core and non-core risks. Core risks are those that banks must take to drive performance and long-term growth. Non-core chances are often not essential and can be minimized or eliminated.

Risk Assessment and Measurement

Risk measurement provides information on the quantum of either a specific risk exposure or aggregate risk exposure and the probability of a loss occurring due to those exposures3. When measuring particular risk exposure, it is essential to consider the effect of that risk on the organization's overall risk profile.

Some risks may provide diversification benefits, while others may not. Another important consideration is the ability to measure exposure. Some risks may be easier to measure than others. For example, market risk can be measured using observed market prices, but measuring operational risk is considered both an art and a science[4].

Specific risk measures often have a Profit and loss ("P/L") impact if there is a small change in that risk. They may also provide information on the volatility of the Profit and Loss Statement prior to reporting dates. For example, stocks measure equity risk based on movements in various

[3] Risk Management Framework: An Overview
[4] Risk Management Framework: An overview

indexes such as S&P 500 index or the standard deviation of the particular equity. Common risk measures include value-at-risk (VaR), earnings-at-risk (EaR), and economic capital. Banks may use such techniques as scenario analysis and stress testing performed by machine learning or artificial algorithms with base line and industry consensus to produce one or two forecasted paths and the effects on financial reporting, for comparability to other banks. However, using a multiversity of possibilities based on "shocks" and unusual events would better forecast economic outcomes and increased risks such as the current economic impact due to COVID-19 pandemic.

Risk Response and Mitigation

After categorized and measured its risks, a company can then decide on which risks should be eliminated and how much of their core risks it can accept. Risk mitigation can be achieved through an outright sale of assets or liabilities, hedging with derivatives, or diversification, etc.[5].

Risk and Control Monitoring and Reporting

It is important to regularly report on specific and aggregate risk measures to ensure that risk levels remain at an optimal level. Financial institutions that trade daily will produce daily risk reports. Other institutions may require less frequent reporting. Risk reports must be sent to risk personnel who have that authority to adjust (or instruct others to change) risk exposures.

As part of the risk and control reporting a forensic accountant can conduct fact finding investigations, analyze alleged fraud or financial mismanagement; review data and advise on current exposures with recommendations for controls, that prevent and detect issues before they occur.

1.3 Organizational Risk Management Governance

Risk management governance is an organizational approach to risk management. It involves applying sound governance principles to identification, measurement, monitoring, reporting, and controlling of risks. It also ensures that risk-taking activities are in line with the bank's strategy and risk appetite.

[5] Risk Management Framework: An overview

Principle 1: As part of an organization's governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the board of directors' and senior management's expectations regarding managing fraud.

Risk governance is the process that ensures all company employees perform their duties following the risk management framework. Risk governance involves defining the roles of all employees, segregating duties, assigning authority to individuals, committees and the board for approval of core risks, risk limits, exceptions to limits and risk reports, and general oversight[6].

Effective risk governance helps ensure that risk management practices are embedded in the enterprise process and, enabling it to secure optimal risk-adjusted return[7].
Risk related information should be disseminated under a structured governance environment. The Board of directors should encourage a holistic enterprise strategy, which then passes to the senior managements to incorporate into the strategic plans. Senior management strategic plans should then pass down to business and risk management units respectively. Through the Risk reporting process, the business and risk management units, the boards and senior managements should align objectives to better balance strategy, risk, and performance.

1.4 Effective Risk Management

A practical risk management approach would encompass controls with objectives to prevent, detect, and respond to a risk threat in a proactive way. However, it's imperative for an organization to understand various regulatory and evaluative frameworks applicable to them and to ensure that adequate internal controls, code of conduct, ethics and compliance procedures that manages and integrates risk prevention, detection and response efforts are in place[8].

- Effective risk management establishes the corporation’s culture which will invariably enable management to enhance competencies, add competitive advantage, and sustainable business model

[6] Risk Management Framework: An Overview
[7] ISACA: Certified in Risk and Information Systems Control Manual (CRISC) 6th Edition.
[8] Fraud risk management KPMG Forensic 2014

- Effective risk management strives to integrate risk management approaches in a manner consistent with legal, regulatory requirements and alignment with its objectives and marketplace expectations.

Most organizations are faced with global challenges about how to develop a comprehensive strategy that will help them align the key objectives of risk management with key tools to manage and mitigate risk in a manner consistent with various standards, regulations, and the business goals.
A comprehensive strategy may be facilitated by enterprise risk management specialists who can assess, design, implement and analyze gaps analysis.

Assessment
The organization needs to assess its enterprise risk management framework and determine the effectiveness and efficiency in the context of the three objectives: prevention, detection, and response with a holistic approach.

Design- Management must develop an effective internal control that will enable them to proactively prevent, detect, and respond to fraud and misconduct risks. Management's decision on control design should reflect its risk objectives criteria and not just merely observing regulatory requirements.
Implementation- Effective and proper implementation strategy and procedures are crucial after the controls have been designed to achieve enterprise risk management objectives: prevention, detection, and response and requires training on corporate culture and practices throughout the organizational.

Evaluation- An existence of a control does not guarantee that it will operate as intended. Therefore, management needs to perform an ongoing gap analysis to determine whether the controls indeed incorporate the three enterprise risk management objectives, as stated earlier, to achieve optimal effectiveness.

SECTION 2

IMPLEMENT AN EFFECTIVE RISK MANAGEMENT STRATEGY.

2.1 Roles and Functions of Bank

The business of banking has changed over the years incorporating new lines such as Wealth Management, Capital Markets, Treasury, Self-investing, Global Asset Management and Insurance According to Armstrong, and Mark Zelmer's article in the Financial System Review 39 "An Overview of Risk Management at Canadian Banks," an essential consequence of this shift has been an increase in the exposure of banks to financial markets due to their increasing size, complexity of transactions and a diverse range of risks.

Canadian banks, just like any other banks, have always faced credit risk, market risk, liquidity risk, and operational risks, among others. But the underlying complexity and importance of certain risks have increased as a result of market pressures and the business strategies adopted by the banks, according to the financial system review. For instance, market risk has grown in importance and has become more complicated to manage, and consequently, back offices and other parts of the banks are facing challenges in keeping up with the pace of innovation in front offices. According to financial system review, part of this complexity arises from the growing importance of very complex legal documentation governing transactions, as well as from issues of whether the trade on the books matches the business outlined in the confirmation.
Banks in Canada have been continuously recognized as amongst the soundest and safest across the globe. Darcy Ammerman and Alex Ricchetti have stated in Banking Regulation 2019 that the global financial crisis, has led to significant regulatory changes (most notably in the areas of liquidity and capital) and were designed to reduce the risk of another global financial crisis occurring and ensures that Canadian Banks will continue to be well-positioned.

2.2 Regulatory Architecture: Regulators and Key Regulations.

The Parliament of Canada has legislative authority over Banks in Canada and are the issues of paper money. The first piece of legislation that governs banking in Canada is the Bank Act 1 and its regulations, while various laws supervise banks in Canada, the office of the Superintendent of Financial Institutions (OSFI) is responsible for prudential regulations. The Financial Customer

Agency of Canada (FCAC) accountable for customer protection. OSFI regulates and supervises all banks under its supervisory framework, develops and interprets legislation, and issues guidelines.

FCAC's Enforcement Division investigates and evaluates possible concerns and has the power to enforce compliance. Other regulatory bodies involved in regulating banks in Canada are the Department of Finance who develops and implements financial sector policy and legislation. The Banks of Canada- federally owned- helps to keep the inflation rate low, promotes efficient banking systems, is responsible for the currency, and also serves as a fiscal agent for the government. The Canada Payment Association- d.b.a Payment Canada (PC); The Canada Deposit Insurance Corporation (DCIC) and The Financial Transactions and Reports Analysis Center of Canada (FINTRAC), to mention but few, helps to protect Canada's financial system by writing regulations detecting and deterring money laundering and terrorist financing under proceeds of crime (Money Laundering) and Terrorist Financing Act and its legislations.

The Ombudsman for Banking Services and Investments (OBSI) is an independent and impartial body that resolves disputes between banks and their customers, where the former is not able to resolve the dispute internally. The Canadian Bankers Association, in its capacity, ensures Canada has a thriving banking system by advocating for effective policies and working with banks and law enforcement to protect Canadians against financial crimes, according to global legal insight 2020. The office of the Privacy Commissioner of Canada has the power to investigate complaints, conduct an audit, and pursue court actions. Finally, the Financial Institutions Supervisory Committee (FISC), whose membership consists of OSFI, the Bank of Canada, the Department of Finance, CDIC, and FCAC, meets to discuss, coordinate, and advise the federal government on issues related to Canadian Financial System.

Lastly, three supranational regulatory bodies are influential in Canadian banking. 1). The Bank of International Settlements (BIS) leads global regulatory work on Financial Systems across the globe. 2). The Basel Committee on Banking Supervision (Base Committee), who is a member of BIS members, of which the Bank of Canada and OSFI are members, sets out to strengthen worldwide banking through the release of recommendations enhancing financial stability. 3).

The Financial Stability Board (FSB) consists of G20 countries, monitors and makes recommendations related to the global financial system[9].

2.3 Relevant Frameworks and Regulations:
{COSO Frameworks (2013 & 2017), COBIT 2019, FAFT, FINTRAC & FINCEN}.

2.3.1 COSO 2013 FRAMEWORK

The 2013 COSO framework was updated in 2017 to provide a comprehensive design over the governance, strategy, and performance of an entity to sustain profitability and prevent fraud. The 2017 COSO framework arose from the increased complexity of business transactions, the evolving regulatory environment, rising stakeholder expectations of accountability and competency, market volatility, and, most importantly, incorporates risk in both the entity's strategy-setting process and driving performance.

The 2013 COSO Framework Components and Principles Guidance comprises five components (consist of 17 principles and 81 points of focus). These principles associated with five internal control components or fraud risk management and provide clarity for the user in defining and implementing an internal control system and understanding of underlying requirements for effective internal control systems strategic goals and objectives. The COSO 2013's original principles are still relevant, viable, and are explained below.

The Control Environment.
The first principle champions ethics and integrity in the corporation, the independent role of the board, and delineates management role in creating structures and reporting lines, which includes the hiring of qualified, competent, accountable employees to achieve its mandate. The Control Environment aligns with the Fraud Risk Management Program's first principle of embedding integrity and ethics, commonly known as the tone from above, the values and code of conduct.

[9] Global Legal Insight 2020

Contrarily, drivers of misconduct can incentivize, reinforce, and spread troubling behaviors that bring about fraudulent activity.

Risk Assessment

The second COSO 2013 principle of enterprise risk management is a core focus that targets the top risks and weaknesses of the organization and determines how to balance their strategic opportunities with risk discipline. Management practices should ensure forward-looking risk assessment practices are maintained throughout the business and new business initiatives. Overarching risks in the financial industry include credit, market, liquidity, insurance, operational, regulatory compliance, strategic, reputation, legal and regulatory environment, competitive, and systemic risks. Canadian banks are continuing to undergo tremendous technological innovation and face top risks such as (i) Information technology (IT) and cyber, (ii) privacy and data theft (iii) Geopolitical Uncertainty, (iv) Canadian Housing and Household Indebtedness and (v) legal and regulatory risk. There are also emerging threats, including digital disruption, climate change, and the challenging new post-COVID-19 pandemic world of business.

The COSO 2013 Fraud Risk Management Principles recommends the performance of comprehensive fraud risk assessments to identify fraud schemes and risks, evaluate existing controls, and implement mitigating controls.

Control Activities

The third principle of the COSO 2013 framework provides for the selection and development of controls over the entity's operations, technology, policies, and procedures to sustain its corporate objectives. This principle corresponds to the Fraud Risk Management Principles, which states that the organization should develop preventative, detective, and mitigation controls to reduce the risk of frauds not being detected promptly.

Information and Communication

The fourth principle of the COSO 2013 framework ensures the timely and effective use of quality information internally moving both upstream and downstream through the organization and then externally to stakeholders such as customers, suppliers, regulators, and shareholders to support the internal control functions. Communication aligns with the fourth Fraud Risk Management Principle, which incorporates a robust communication practice directed to address, identify, and prevent fraud in an appropriate and timely manner. Also, Ontario's Securities Act (2016) established a Whistle Blowing program for those who may be aware of corporate misconduct and decide to go public. These confidential calls require the entity to have separate reporting lines in place.

Monitoring

Risk monitoring and reporting are critical components of the COSO framework, which support management and the Board in their oversight role. Monitoring also provides data for regulatory compliance. Some of the tracked monitoring information includes the top risks and emerging risks, portfolio quality metrics, and all management's corrective actions.

The fifth Fraud risk management principle advised the entity to perform ongoing evaluations to ensure the five fraud risk management principles are functioning as intended. In the dynamic and volatile banking industry, processes and controls can shift quickly, as well as market conditions, leading to an increase in fraud schemes.

One current example is the COVID-19 pandemic, which has impacted bank staffing, reduced business hours, created higher online usage, disrupted supply chains due to transportation restrictions, closed non-essential businesses, putting stress on working capital, credit products, and providing emergency business loans. Currently senior management has a higher duty and responsibility for safely delivering higher value, more transparency, and accountability over financial results and security over data and privacy. Canadians have reportedly experienced potential COVID-19 scams and cyber threats involving websites, emails, texts and calls to capture personal information and to access their funds. Financial institutions have been facing

heightened risks unlike any seen before and it is a real-life test of their risk management frameworks.

2.3.2 COSO 2017 FRAMEWORK

The newly updated COSO 2017 framework, entitled Enterprise Risk Management- Integrating with Strategy and Performance, encompasses the following:

- It provides greater insight into the value of enterprise risk management (ERM) when setting and carrying out the strategy.
- Enhances alignment between performance and ERM to improve the setting of performance targets and to understand the impact of risk on performance.
- Accommodates expectations for governance and oversight.
- Recognizes the globalization of markets and operations and the need to apply a common albeit tailored approach across geographies.
- Presents new ways to view risk to setting and achieving objectives in the context of greater business complexity.
- Expands reporting to address expectations for greater stakeholder transparency.
- Accommodates evolving technologies and the proliferation of data and analytics in supporting decision-making.
- Sets out core definitions, components, and principles for all levels of management involved in designing, implementing, and conducting ERM practices.

The COSO 2017 integrated framework incorporates strategy and performance, segregates enterprise risk management from internal controls, and follows the business model versus remote risk management. The following table from the COSO 2017 framework introduces 20 Risk Management Components of 5 key Principles.

Source: COSO 2017 Enterprise Risk Management Framework: Integrating with Strategy and Performance Introduces Principles 20 key principles within each of the five components, Pg 17.

Here is a brief overview of COSO 2017 and comments on some of the new principles. The first component of COSO 17, Governance and Culture defines Principle 3: Desired Organizational Behaviors***:*** describes the corporation's culture and drives how the organization applies the framework. Values such as open communication and leadership style help to identify critical risks and decide if they are accepted, avoided, or reduced and how they will be managed.

Principle 4: Demonstrates a commitment to core values. This is a change from COSO 2013, which referred to "demonstrating a commitment to integrity and ethical values." The new reference to culture calls for a loud tone at the top and a code of conduct that prompts management to align business objectives to the entity's mission, vision, and values. It ensures management and the Board have an opportunity to define the desired culture, review the implications to the entity's strategy, and the risks that result from executing the selected plan.

The second component of COSO 17, Strategy and Objective-Setting replaces the COSO 2013 Risk Assessment, and has updated the elements to include Principle 6: Analyzes business context, Principle 7: Defines risk appetite, Principle 8 Evaluates alternative strategies, and Principle 9: Formulates business objectives. The business context refers to management's consideration of the economic environment and stakeholders' requirements when designing their approach to supporting their mission, vision, and core values. The business context impacts the entity's risk profile and may be viewed in three stages as past, current, and future performance.

The third component, performances, lists Principle 10: Identifies Risk, which is those risks that arise from the execution of strategy and business objectives. Management identifies top risks, emerging threats, and changing risks that result from the achievement of strategy and business objectives, as the business objectives or business context change and refine the risk profile.

Principle 11: Assesses Severity of Risk: The organization risks are assessed and reviewed for the severity of each risk, which may impede the achievement of an entity's a strategy and business objectives. The entity may use qualitative, quantitative approaches, including scenario analysis, simulation, data analysis, and interviews. Management will then make decisions and allocate resources to mitigate the appropriate risk response.

Principle 12: Prioritizes Risk: The entity reviews the risks, according to metrics such as adaptability, complexity, velocity, persistence, and recovery. The entity prioritizes risks at all levels and then prepares responses to risks.
Principle 13: Implements Risk Responses: Once the risks are prioritized and decisioned, management will consider criteria such as the business context, cost-benefit impacts, obligations and expectations, risk severity, risk appetite, and the appropriate risk responses.

The fourth component is Review and Revision, which is centered on reviewing the strategy, business objectives, and ERM practices. The banking industry can be dynamic, volatile, and agile to adapt to new environments, disruptions shifting business context and management, and the board to be aware and able to assess and implement mitigation techniques to ERM.

The fifth component is Information, Communication, and Reporting, which is an iterative process of sharing information both internally and external to the entity. The entity may report on risks, culture, and performance throughout the entity.

These five components represent the business processes which the entity follows to combine business objectives, strategy, implementation, and the day-to-day performance monitoring to enhance ERM and results.

2.3.3 COBIT 2019 FRAMEWORK - DRIVERS AND BENEFITS FROM A RISK PERSPECTIVE

ISACA, the main driver for the new COBIT 2019 describes components parts for decision making in its Framework for Enterprise Governance of Information and Technology (EGIT) updated from the COBIT 5. This update was to address gaps, new technologies and business trends in IT (e.g., digitization, new paradigms), and provides insights from business, as a result of the constant evolution of standards, frameworks, and regulations.

The reforms, the COBIT 19 framework, identified a new design for the Enterprise Governance over Information and Technology and Business/IT alignment as the means to create value.

The ISACA Risk Event of April 11, 2019, has provided its goals as:

- COBIT 2019 integrates risk governance and management with overall I&T governance and management.
- COBIT 2019 provides the hooks for more detailed and technical guidance beyond the scope of COBIT 5.
- COBIT 2019 includes integrated process capability assessments, based on CMMI.
- COBIT 2019 updated the generic risk scenario to support management efforts.
- The COBIT 2019 Core Model contains specific risk governance and management objectives and includes supporting processes such as (i) EDM03-Ensured Risk Optimisation (which continually evaluates the effects of risk in I&T and risk appetite using critical metrics related to the enterprise value), (ii) APO12—Managed Risk (which develops a substantiated view of actual I&T risk in support of risk decisions, measure with critical metrics and (iii) Specific Organizational Structures, Skills, Culture aspects, etc.

  The COBIT 2019 Risk Profile Design Factors of IT Risk Categories identify and indicate where there is risk exposure, and it exceeds the entity's risk appetite. They are listed as

  (i) IT-investment decision making and maintenance - which includes such risks as being misaligned with corporate strategy, IT investment failure in support of

digital strategies, and failed performance structures for implementation, which may be related to cost, performance, and incompatibility to other systems.

(ii) Programs and Projects for lifecycle management- examples include failure of senior management to terminate an unsuccessful project due to changes in business priorities or budgets, or failure for third party contractors to deliver as per contractual agreements.

(iii) IT cost, and oversight – lack of funds for IT related investments in a start-up, small requirement gathering leading to ineffective service level agreements.

(iv) Logic Attacks (hacking and malware) include risks related to foreign government attacks on systems, unauthorized breaking into the IT system, denial of service, and data loss by disgruntled or untrained employees.

(v) Third-Party Supplier incidents -include the risk of inadequate performance of the outsourcer in a large-scale, long-term outsourcing arrangement, if sales volumes are low there may be unreasonable terms and invoicing from IT suppliers, inadequate support not align with service level agreements, and the overreliance on the current supplier creating an inability to transfer to other vendors. And lastly, possible breaches on the vendor's IT systems which may affect SLAs and open vulnerabilities.

The Risk profile will also include an assessment for risks that have recently materialized, or where the entity is currently facing results such as a low contribution to business value, failed initiatives, or failure to meet or implement new regulations. One such new regulation is the vast changes required to amend the regulations to the *Proceeds of Crime (Money Laundering)* and Terrorist Financing Act (PCMLTFA) coming into force on June 1, 2021. Reporting entities will have to move quickly to review and clearly define the requirements from a banking industry perspective, determine the scope of changes necessary to update policies, procedures, and hire skilled staff to build and test the new technology required to implement the changes operationally.

The new COBIT 2019's approach to Risk Management is expected to confront several weaknesses noted in COBIT 5, such as the fragmented manner in which Risk Management has

been organized in the past, the historical lack of senior management involvement in the conflict between risk management and performance, the inconsistent methods used in identifying risk and risk assessment as a result of unclear taxonomies and vaguely defined risk appetite.

Most notably, the COBIT 2019 reflects the ideology of the COSO 2017, which serves to enhance business leaders' understanding, recognition, and prioritization of the risks their organizations face and transparently measure how these risks impact business performance. It would then be the ultimate responsibility for management to weave together the culture and set incentives commensurate with proper risk management processes that create and maintain value in their portfolios.

2.3.4 FATF, FINTRAC, and FINCEN

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops policies to protect the global financial system from financial crime, money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction[10]. The FATF 40 Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard, as pointed out in 2012-2019 FATF/OECD (Appendix 2).

The mandate of the FATF is to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing, financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities to protect the global financial system from misuse[11].

Financial Transactions Reports Analysis Centre of Canada (FINTRAC) and Financial Crimes Enforcement Network (FINCEN) was established to fight against money laundering and terrorist financing in Canada and the United States, respectively. (see appendix 8 for FATF 40 Recommendations)

[10] International Standards on Combating ML/FT and proliferation updated June 2019
[11] International Standards on Combating ML/FT and proliferation updated June 2019

The FATF updated 2016 Standards strengthen the requirements for higher-risk situations, and to allow countries to take a more focused approach in areas where high risks remain, or implementation could be enhanced.

Every country's laws differ and therefore, the FATF recommendations set an international standard that countries should implement according to the measures adapted to their financial environment. The FATF recommends the following policies be adopted:

- identify the risks, and develop policies and domestic coordination
- pursue money laundering, terrorist financing, and financing proliferation
- apply preventive measures for the financial sector and other designated sectors
- establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures
- enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
- facilitate international cooperation.

The FATF's mandate after 30 years continues to be recommending the adoption of legal, regulatory and operational measures to prevent emerging threats, and weaknesses in the global financial system that opens vulnerabilities to money laundering, terrorist financing that would prevent the integrity of the international financial system.

2.4 Forensic Accountant Interaction with Regulations and Standards

A forensic accountant would add value in reviewing the new AML regulations from FINTRAC, to identify and anticipate the data collection, reporting and controls that would the detect risks of ML/TF and ultimately add competitive advantage to risk management functions as summarised below:

- Forensic accountants are trained to analyze the regulatory standards, review the profiles of senior management, the corporate culture, the processes, and controls in the lines of

business (account portfolio) in comparison to the applicable Risk and controls (FINTRAC AML Regulations) and systems under which each branch and correspondent bank operations.

- The FAs have professional accounting skills and this may include the ability to : (a) identify, trace and evaluate the property that is subject to confiscation; (b) carry out provisional measures, such as assets freezing and seizing to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures;

- FAs, while analyzing customers' behavior that may be associated with a white-collar crime, can help banks develop relevant and enhanced customer due diligence where it is possible to anticipate possible motivation and intent.

- FAs understand the importance of the objective investigation, practice skepticism, are trained to document, record, manage research into standards and legislations, handle evidence and write reports, as they are experts in conducting investigations into fraud. FAs can compare various types and sources of information to review and investigate a portfolio of transactions, purposefully design scope, and overall conduct of the portfolio investigation to ensure objective and thorough outcomes.
- FAs can develop an overall strategy of risks identification, and investigation of the main concerns related to the nature and scope of the testing;
- When FAs learn the issues, they can develop the scope of work (investigation) to be performed, with the following considerations in mind:
    i. develop hypotheses as to what might have occurred based on the known facts that will help FA determine what type of evidence to be elicited and the analysis to be performed.
    ii. identification of approaches, procedures, and techniques needed to accomplish the investigation objectives effectively. Procedures may include, but not limited to, account reconstruction, preparation of source and use of funds, asset tracing, and net worth analyses- to reflect evolving ML/TF trends and techniques to uncover any potential risks

- FA can help banks identify, assess and understand any potential risks of ML/TF and adopt appropriate reactive, preventative risk-based measures to mitigate those identified and evaluated risks
- Based on identification and assessment of the risk, FA will adopt and apply a risk-based approach (RBA) techniques and framework to ensure that measures to prevent or mitigate ML/TF are commensurate with risks identified and aligned with FATF AML/TF framework (FATF Recommendations) as amended.

In the Standard Practices for Investigative and forensic accountants' section 100.15, it states that "At its boundaries, a skills-based definition for IFA engagements will likely overlap with definitions for other disciplines, such as assurance, information technology, business valuation, corporate finance, tax, private investigation, and insolvency and restructuring." In consideration of this statement, the FA's skills could also include Enterprise Risk Management and data analysis.

SECTION 3

OVERLAPPING SKILLS BETWEEN RISK MANAGEMENT SPECIALIST AND FORENSIC ACCOUNTANT

Obviously, some skills mentioned below overlap between forensic accountants and risk management experts due to the distinct characteristics of the two professionals as it relates to risk management functions. However, either might view the same concept or point from different perspectives. Forensic accountants might view from the legal point of view while risk management analysts view it from management point of view.

3.1 Required skills for Risk Management Specialist

Simply put, risk management is being aware of what could go wrong at any time, decide if those risks can be managed or not and how they would affect the business or taking actions to avoid either problems or its consequences when risks eventually occur. Risk management can be interpreted as an act of art and science; therefore, risk management officers should possess a range of unique skills, knowledge, and qualities across the board.

Analytical risk assessment skills

It is evident that to assess and predict risk, you must have analytical skills, but it goes further than that. Another key element is taking the data and seeing any potential gaps to conduct further research. Therefore, a risk management officer must have a desire to take things further to get a clearer picture.

Problem-solving

If potential risks are found, you must be curious enough to look at the business issue and get to the crucial solutions. If you have a desire for effective problem-solving, you'll be able to push for the real answers and strategically look for solutions.

Strategic thinking

If you like thinking about how things affect all areas of business operations and can look at all possibilities, you are likely more able to come up with solutions as well as look at opportunities. Risk management officer should be able to see the big picture, then break it down and find solutions and opportunities.

Financial knowledge and skills

All businesses have some element of financial risk – often, the numbers can be quite scary! A good risk management officer can identify and measure the risk and implement strategies to mitigate those risks. If you can determine which risks can be managed versus which risks are beyond your control, you can focus on contingency plans and prepare for the unknown.

Regulation Update

It is exceptionally vital that risk management officers invest the time to stay ahead, skill up, and understand all regulation changes and updates. Great risk managers must tackle regulation updates with the seriousness that it deserves with the skill and ability to research databases.

Ability to build relationships

Risk management officer must be good at relationship building because, to look at and manage risk, he/she will have to manage relationships between several different departments and other stakeholders.

Working under pressure

Managing risk is inherently stressful; it means managing huge issues, problems, and solutions often have genuine and expensive issues if not contained. Having systems in place, and planning strategically, can help risk management officer to mitigate the stress involved.

Communication & presentation skills

Risk management officers should have the ability to produce risk reports, attend meetings, and present your proposals to other senior members of the management team or the board succinctly.

Adaptable to new concerns and changing environments

Risk management officers must get acquainted with new political, financial, and professional environments. As an (RMO), each day brings new concerns leading to changing settings in which business operations are performed. Many years ago, managers didn't need to worry too much about cyber-attacks. Data breaches, ransomware, and cyber-security and malfunctions are real risks in business, especially in the banking industry.

3.2 Required skills for Forensic Accountant

Forensic Accounting:

Forensic accounting is the specialty practice area of accountancy that describes engagements that result from actual or anticipated disputes or litigation. Forensic accounting means to be used in or suitable to a court of law, of judicature or to public discussions, debate and ultimately dispute resolutions, it is also defined as an accounting analysis that is suitable to the court which will form the basis for discussion, debate and ultimately dispute resolution.

Forensic accountants require a multidisciplinary knowledge of accounting, law, psychology, business, criminology, and information and communication technologies (ICTs); and also has critical thinking ability; systems thinking ability; emotional intelligence; knowledge of fraud schemes; discernment (ability to read character or motives; a searching mind that goes beyond what is visible or superficial; and the ability to recognize subtleties in thoughts and motives, among other qualities.

According to Kevin Shergold (2018), forensic accountants are integral to the performance of a modern financial investigation[12]. Forensic accountants may be involved in recovering proceeds of crime and about confiscation proceedings concerning actual or assumed proceeds of crime or money laundering. Some forensic accountants are Certified Fraud Examiners, Certified Public Accountants, Certified Anti Money Laundering Specialists, or Chartered Accountants. Forensic accountants utilize an understanding of business information and financial reporting systems, accounting and auditing standards and procedures, evidence gathering and investigative techniques, and litigation processes and procedures to perform their work.

Crumbley defined Forensic accounting as the action of identifying, recording, settling, extracting, sorting, reporting, and verifying past financial data or other accounting activities for resolving current or prospective legal disputes or using such past financial data for projecting future financial data to settle legal disputes. This definition supports the preceding statement about the forensic accountant. FA experts can be critical in a variety of matters: asset misappropriation, bribery and corruption, money laundering, competition infringements, employee misconduct issues, regulatory breaches, market abuse, cybercrimes, commercial disputes, and even acute investment or value decline.

The value of forensic accountant/investigator

According to "The European, Middle Eastern and African Investigation Review (2018), Kevin Shergold stated some attributes that make forensic accountant investigators so additive in supporting and adding value to internal investigations and risk management functions as follows:

- an understanding of the accounting and control environment that surround transactions;

[12] Grant Thornton UK LLP- GIR

- an ability to appraise the commercial imperatives for different actors in the purchase and sales cycles;
- an understanding of where the repositories for evidence will be found and how to mine them;
- a well-practiced forensic discipline of ensuring findings are objective and re-performable, applying the most advanced technology; and
- the ability to build the factual narrative amidst the inevitable gaps in information.

To further reiterate the value of forensic accountant in investigation procedures or processes, Kelvin asserted.....

"I recall coming into an investigation at a very late stage, where the legal team had focused its attention on the emails of, and interviews with, a broad set of senior and middle managers in response to sanctions breach allegation. Despite consuming a whole lot of time and resources, progress was slow. The case turned on a redirected focus over two small departments' activities in a subsidiary in Eastern Europe – the IT team and the finance function, following our assessment."

It is obvious risk management analyst and forensic accountant have similar skills. However, following skills listed below distinguish a FA from risk management analysts. This indicates that a forensic accountant will add value to risk management functions as team member of specialists to mitigate risks because of these peculiar skills.

Understanding of Business Entity

Forensic accountants have an innate understanding of business setups, types of businesses, and regulations behind the structure and not just related to transactional records and accounting ledgers but to processes, controls, records, people, departments, decisions, and strategy. FAs place in the bigger picture is discernible.

Communication & Reporting Skill

Ability to communicate well both verbally and in writing is necessary to obtaining information, directing, presenting findings, and achieving desired results. The integrity and validity of such information communicated will be guaranteed because the IFA practitioners confined their

findings and conclusions to the subject matter, principles, and methodologies within their competence, including knowledge, skill, experience, training, and education acquired.

Advanced Computer Skills

This skill helps forensic accountants to dissect unstructured data that does not readily conform to a database or spreadsheet format. The text associated with messages in emails, explanations for journal entries, and other communications are the most common examples. Unstructured data also includes photographic images, video, and audio files. Such skills will also help forensic accountants to detect when a user 'deletes' electronic information. This is because a back-up or archive version is often left behind and is available to an investigator. Understanding an organization's back-up, archiving, and storage practices are crucial for a forensic accountant to effectively add value to the organization's risk management function and an investigation. The concept will be discussed further under how a forensic accountant can add sustainable value.

Mathematics and Statistical Skills

Forensic accountant's ability to build on the foundation of probability and statistical theory to help identify financial fraud by applying mathematical tools is imperative in adding sustainable value to the bank's risk management functions. Effective FAs skills based on intuition, conjecture, and experience acquired over time helps in a great deal to uncover created fraud and patterns of fraud.

Problem Solving Skill

Ability to review the internal control weakness and highlight the weaknesses found could have led to potential fraud. Forensic accountants must have impeccable problem-solving skills to determine how a crime was committed. They are often involved in a case after a fraud has already occurred and thus must puzzle out all the different aspects of the crime.

Data Analytics& Data Mining Skills

With the exponential rise in automation, there are increased pressures and expectations for an IFA to be more focused on interpreting and analyzing the data. Therefore, the ability to gain real-time visibility into status, progress, exceptions, and risk points is an essential tool for forensic accountants, especially knowing what to measure and where to start.

Data normalization and structuring Skill

A forensic accountant has acquired the necessary skills needed to normalize and structure all collected data, so it can be linked, as it may originate internally or from third parties. Some will be structured, such as that arising from databases, while others will be unstructured, such as text-heavy data. Only when data is normalized and structured will you derive all possible insight from the information you have collected.

Legal environment Skill

This is the forensic accountant's ability to gain a thorough understanding of statutes, standards, rules, and regulations and keep abreast of any changes as it may affect the work of a forensic accountant. It is also an ability to critically analyze and interpret relevant criminal and civil laws pertaining to forensic accounting and fraud. FAs also gain a thorough understanding of the rights of the parties involved in allegations of occupational fraud and the rules of evidence and its applicability.

Expert Witness Skill

Section 700.02(a) of standard practices for investigative and forensic accounting engagements, states that forensic accountants must provide independent assistance to the Tribunal by way of objective, unbiased testimony with matters within their expertise.

Interviewing Skill

In the context of a fraud risk investigation, such skills are vital when facing the ethical, legal, and psychological challenges of a suspect interview. With proper training and practice, forensic accountants possessed skills that assist them in shaping optimal investigative outcomes.

Therefore, the importance of excellent interviewing skills cannot be underestimated[13]. For investigations where no documentary evidence is available, interviews are the only way to gather evidence; interviews alone may not lead to a definite resolution of the case[14].

Investigative mindset and Investigative Skills

Forensic accountants have good investigative ability and investigative intuitiveness to synthesis results of discoveries and analyze them. Often the people who commit fraud are simply opportunists, taking advantage of a weakness or absence of control. If FAs hopes to prevent fraud, they must identify the opportunities before fraud takes place and address any weaknesses in the controls. The ability to trace the assets in a bid to recover what was stolen is also imperative for an IFA to successfully add a competitive advantage to the bank's risk management functions. For example, in an engagement to develop fraud risk prevention policies, an investigative mindset is applied to establish the process for determining ways in which policies could be violated or compromised[15].

3.3. The role of Forensic Accountants Vs. Traditional Financial Accountants In Banking Sector Risk Management.

The published Sarbanes Oxley incorporates concepts and procedures to deter and to catch fraud in audits of internal controls over financial reporting. However, the focus of financial audits and financial reporting ultimately is concerned with providing reasonable assurance that a material misstatement to financial statements has not occurred, regardless of the reason. Also, failure of statutory audit to prevent and perhaps mitigate misappropriation of corporate fraud, inadvertent increase in corporate crime, and gradual eroding of public confidence in financial statement and reporting has called for a better ways of exposing frame in business world by shifting paradigm to a forensic accountant to drill down the fraud and risk investigations.

[13] Journal of Forensic & Investigative Accounting 2012
[14] MFAcc IFA 2905H Material: Interviewing Skills
[15] MFAcc Program IFA 1900H: Forensic Accounting & Investigation, Fraud & Cybercrime Material(2017)

While it is true that many of the financial statements and frauds could have, perhaps should have, been detected by financial auditors, the vast majority of frauds could not be identified with the GAAS of financial audits. Reasons being traditional financial auditors' dependence on a sample and the reliance on examining the audit trail versus forensic auditors' examining the events and activities behind the documents. The latter is simply resource prohibitive in terms of costs and time.

Forensic fraud auditors look beyond the transactions and audit trail to focus on the substance of the transactions instead. Forensic fraud auditor doesn't question if there is a prudent internal control in place. It does not ask if the accounting process complies with the accounting standard, either as traditional accountant would. But it rather questions about:

I. Where are the weakest links in this system's chain of controls?
II. How are off-balance sheet transactions handled, and who authorizes and approves such transactions?
III. What could control features in the system be bypassed by the higher authorities?
IV. What are deviations from conventional good accounting practices possible in the system?
V. What are the nature of the work environment and the tone at the top?
VI. What would be the simplest way to compromise the system?

Traditional fraud audit involves a specialized approach and methodology to discern or detect fraud; that is, the auditor is looking for evidence of fraud with a single purpose to prove whether fraud exists or not. Whereas, forensic fraud investigation or audit usually encompasses the same thing as a traditional financial audit except that forensic investigation typically involves a lot more non-financial forensic evidence, such as testimony from interviews, than a fraud audit.

A forensic accounting engagement is designed and explicitly conducted to uncover fraud. The objective often is to determine who committed the fraud, how it was perpetrated. How much was involved and how to prevent such occurrence.

A forensic audit is more encompassing than a financial statement audit in terms of assessing the entity's internal control structure and identifying alleged fraudulent activities or irregularities. While forensic engagements follow the basic rules prescribed under GAAP, it may depart from

all or parts of what is stated under GAAP depending on the circumstances. In other words, there are no set guidelines or rules when it comes to forensic accounting engagements (Principle-based) compared to traditional financial audits/engagements (Rules-based).

Forensic accountants will generally start with analyzing the company's financial statement data and then proceed to other procedures to unveil specific circumstances or a series of events that have occurred to enhance risk management functions.

The forensic accountant will interview a wide range of personnel, from the clerical staff to the senior management, as the case may be. Based on these interviews and other observations, the examiner will start to identify red flags and design follow up procedures to address the suspicions and/or high-risk areas within the organization.

"A forensic audit report of findings is a fact-based document that may detail internal control weaknesses, alleged acts of malfeasance, and the magnitude of the alleged loss." In certain circumstances, the forensic audit report may even include a recommendation to improve the identified weakness or gaps in internal controls.

The forensic audit report can have many purposes, including use by an entity’s management to seek restitution from the alleged perpetrator, use by management to strengthen internal controls to prevent fraud from occurring in the future, or use by law enforcement to bring criminal charges.

Each forensic project is unique and may require the forensic accountant to develop an audit program for the specific objective of individual engagement. Typically, the forensic accountant will work with a legal team, and will always work under the assumption that he or she will have to testify as an expert in a court proceeding. The qualifications and expertise of the engagement team are paramount as the documents created during the forensic audit may be needed in civil and criminal proceedings, by law enforcement and government agencies, or confidential investigations.

Forensic accountant's significant contribution under any circumstances is in translating complex financial transactions and numerical data into terms that ordinary laypersons can understand.

That is necessary because if the fraud comes to trial, the jury will be made up of ordinary laypersons.

Forensic accountants are trained to react to complaints from criminal matters, statements of a claim arising in civil litigation, and rumors and inquiries arising from corporate investigations. The investigative findings of the forensic accountant will impact an individual and/or an organization in terms of financial award or loss of their risk management decisions.

Comparisons between Forensic Accounting and Traditional Auditing

Area	Forensic Accounting	Traditional Auditing
Scope	Elaborate on why an occurrence with necessary and conclusive proof	Only focus on ascertainment validity and reliability of financial statements
Technique for obtaining evidence	Observation, Data analysis, interview, Electronic evidence review and preservations	Based on sampling method only
Limitation to use of the report	Mainly for litigation support. Not limited by any standards.	Addressed to the management and board of directors. No further checks are performed due to adherence to standards
Frequency	Whenever there are disputes which may result in litigation	It's produce at least yearly
Purpose	To analyze, summarize, interpret and present complex financial and business risk related issues in a form allowing for litigation processes.	Statutory only

Investigation	Investigate every financial transactions that might be connected with fraud or risk of fraud	Does not investigate
Period of activity	No specific timeline, activity lasts until the fraud is discovered	Expression of opinion on the financial statements for one business year

Source: Adapted from the "MFAcc" study materials (2017)

Forensic accountants presume that audit trail, GAAP or GAAS does not truly depicts or mean that financial recorded transactions are free from fraud. Whereas, traditional auditors rely on financial recorded transactions and audit trail in terms of availability, reliability as supporting documentations and which are not legally bound to authenticate accounting data in the court of law. Unlike traditional auditor, forensic accountant are trained and expected to be an expert in documentation authentication in the court of law. This really explains the difference in forensic accountant and traditional auditor's mindset.

Traditional accountant/auditor skills are intended to provide reasonable assurance that the financial statements are stated fairly in all materiality and in accordance with GAAP, and are therefore, free of material misrepresentations. On the contrary, forensic accountant skills represent skill sets, training and techniques developed to detect and prevent fraud.

Unlike traditional accountants, forensic accountants conducted detailed analysis of data by deploying data-driven techniques to assess possible risks that might be associated with banking transactions. Both forensic and traditional accountants helps monitor big financial data to identify sparks, however, forensic accountant helps banks in preventing reputational damages by preventing loss of consumers' information and privacy

Assessment of fraud risks by applying the forensic accountant mindset and skills will definitely stimulate higher task performance than the traditional auditor mindset and skills in banking risk management functions as depicted in the table above.

SECTION 4

RECENT CASES OF RISK MANAGEMENT FAILURES AT BANKS

4.1 Danske Bank- Estonia Branch, Money Laundering case (2007-2019)

Danske Bank's senior management and the board ultimately failed in its Ethics and Compliance duties, which opened the door to the most significant money laundering failure in Europe, estimated at 230 billion Euros in suspicious transactions funneled through the bank's Estonia branch from 2007 through 2015. All levels of management at Danske bank turned a blind eye to their compliance regimes to advise the board, investigate the identities and transactions of non-resident accounts under the European Union's AML4 directives, accepted faulty AML procedures at the Estonian Branch, and did not seek to comply with the recommendations made by regulators in a timely or responsible manner.

In 2018 Danske bank was ordered by Estonia's regulator to pull out of the country and has been the focus of criminal investigations in Denmark, Estonia, and the United States. Preliminary criminal charges have been brought against several of its former executives in Denmark, including former group CEO Thomas Borgen who resigned due to the incidence (Bradley Hope, Drew Hinshaw and Patricia kowsman 2018). Danske Bank management and the board failed its duty of care required as a fiduciary to "inform themselves" before making a business decision, of all material reasonably available to them." Below are some of the major issues identified:

- The Audit Committee has no risk management responsibilities and operated in silos and did not make the parent company's executives and board aware of deficiencies.
- There was a lack of disclosures regarding allegations of money laundering in the Estonia branch as expressed by Borgen who said, "with respect to Estonia, he had not come across anything that could give rise to concern", according to Caroline Binham and Richard Milne in Financial Times 2018
- There were violations of Danish FSA and Estonia FSA money laundering legislation on the monitoring and operating transactions to and from correspondent banks
- There were violations of section 290.4(2) of code of ethics for professional accountant - an assertion about the effectiveness of internal control (subject matter information)

results from applying a framework for evaluating the effectiveness of internal control, such as COSO or CoCo (criteria) to internal control, a process (subject matter)

- There was a failure to integrate Sampo Bank's Finish activities into Danske Bank's IT platform to align with COBIT 5 for Risk regulations and monitoring of transactions for compliance.
- Danske Bank had no way of knowing how many customers constituted the non-resident portfolio because no customer lists were kept until 2013
- Sampo Bank was permitted to operate as a standalone subsidiary following its acquisition in 2007, even though it was a branch of Danske Bank in 2008 and had officially changed its name to Danske Bank in November 2012
- Conflict of interest - former head of Baltic operations, T. Borgen, later became Danske's CEO and steadily increased profitability and grew the customer base at Estonian branch, mostly from the non-resident business. He dismissed concerns, and failed to investigate Russian transactions in Estonia, and did not follow AML4 regulations for politically exposed persons or beneficial ownership.
- Deficiencies were found concerning "know your customer" (KYC) information regulation.

It is fair to say that Danske bank's routine practice has not been followed by management, the board minimally followed their responsibilities as per COSO 2014, 2017, the regulatory controls were not entirely in compliance with the requirements stipulated in the law and international standards.

4.2 Analysis of the Three Lines of Defence at Danske Estonia's branch.

The first line of defence is with the staff at the business unit level, who should understand the processes, procedures, products, and controls implemented by the Risk Management team. This environment reflects compliance with the board-approved risk appetite. At Danske Bank Estonia, the board directors and top leadership failed to establish the role of enterprise risk management in the setting and execution of strategy and the achievement of performance goals.

The staff's procedures had significant deficiencies in its governance and control systems over non-resident clients allowing Danske Bank's branch in Estonia to be used for suspicious transactions. Investigations led by an external law firm Bruun & Hjejle in 2018 found that staff

had non-arms length connections with customers or enabled them to process suspicious transactions.

The second line is with management and the Chief Compliance Officer. They are responsible for overseeing the bank's risk-taking activities and working with business units to create a compliance management system based on policies, training staff, monitoring activities, and reporting to the Board. Danske board and management were aware of a high volume of suspicious transactions in Estonia, and whether that might complicate the bank's expansion in the Baltic. The suspicious activity increased between 2010 and 2015 without investigation.
Another example of management failure to enforce accountability was by allowing a high-risk operating unit to maintain a separate IT system. The Information systems should have been integrated across Danske Bank Group, which would have produced transaction monitoring through adequate process-level controls and improve transaction-level controls intended to detect suspicious payments. A responsible management team would have budgeted for new and robust IT systems and increased automation of work to ensure compliance and transparency.
The third line of Defence is Internal Audit, which ensures the compliance framework and internal controls are appropriate and adequate to the identified risks. The internal audit evaluates the compliance standards at the business unit level and reports its findings to the board. Danske's internal audit team first audited the Estonia branch in 2011 and gave it a "fair" rating (the third-best out of five) for AML procedures. In 2014 the audit team investigated a whistleblower's report and compliance failures; however, its draft report was never finalized or resolved by the board. The finding deemed that controls over anti-money laundering were insufficient, and the board did not act to resolve the internal audit report.

In 2019 the European Banking Authority (EBA) investigated the Danske case and found that the 2007 and 2013 Russian Central Bank’s warnings on Danske’s non- residents went unheeded. The Russian Central Bank believed Danske’s clients were receiving transfers from Russian shell companies which were not supported by legitimate exchanges of goods or services and were suspected as concealing tax evasion and money laundering.

Reuters reported on April 26, 2019, that the EU's national banking supervisors, who control the EBA, rejected the watchdog's proposal on the rule (of law) breach and effectively blocked further action against the Estonian and Danish regulators. The two regulators from Estonia and Denmark and the Russian Central Bank did not respond to Reuter's requests as to why they did not support legal proceedings against Denmark and Estonia for their flaws in applying EU laws. Leading one to ponder that these two members were not objective and feared additional investigations would lead to more charges and higher fines.

The outcome of such widespread misconduct, as a result of suspicious funds from Russian oligarchs being placed, layered and integrated into the financial system via Nordic banks into the West over several years has been detrimental to Danske's share price. Bloomberg News reported on January 30, 2019 that Danske lost almost 50 percent in market value, and shareholders experienced 25 percent in further declines to share prices 2019. The bank is also facing class-action lawsuits from investors. In May 2019, Danish prosecutors charged Thomas Borgen, former chief executive of Danske Bank, over his involvement in financial crime and money laundering. In February, Estonian regulators told Danske Bank to close its branch in Tallinn before the end of 2019

The Bloomberg article of September 25, 2019, reported that Aivar Rehe CEO of Danske Bank in Estonia between 2007 and 2015, and who was a witness into the investigation of money-laundering was found dead in an apparent suicide in September 2019. The article further reported that "Rehe said that as the CEO of the Estonian branch, he naturally felt responsible for the affair."

The Bruun & Hjejle law firm, in their 'Report on the Non-Resident Portfolio at Danske Bank's Estonian branch (2018)', revealed their investigations of the 2007 to 2015 period reported, "reprehensible conditions at our Estonian branch and Group level allowed Danske Bank's branch in Estonia to be misused for suspicious transactions, and they also showed that we reacted too late and too slowly."

On January 29, 2020, Bloomberg News reported the Danish Business Authority claimed that "Danske's auditors, Ernst and Young, who would face disciplinary action for failing to audit according to generally accepted audit standards (GAAS)." Also had insufficient documentation

and for a failure to detect signs of possible AML at Danske Copenhagen." In May 2020, these charges were dropped.

In 2020, the European Union has recently updated the A Guide to Anti-Money Laundering (AML) Compliance, the AMLD5 follows on the heels of AMLD4. There are directives to be followed - 2.1. Ultimate beneficial ownership (UBO), 2.2. Politically exposed persons (PEPs), 2.3. High-risk third countries, 2.4. Prepaid cards, 2.5. Crypto markets, and 2.6. Monitoring Financial Intelligence Units (FIUs).

The directive on Monitoring Financial Intelligence Units under AMLD5, provides the first line of defence, the ability to "facilitate cooperation and information exchange between authorities. The member states of the European Union must establish national registries for banks so that they can identify all accounts of any person by the corresponding FIU. This is especially encouraging, should staff in the business unit have information of interest they can provide it to the authorities.

4.3 How a Forensic Accountant can help Danske Bank to Prevent or Mitigate the Risk?

What could Danske Bank have done to recover from setbacks to the ERM connection between ethics and compliance risk to accountability and strategy? The parent company could have retained forensic accountants with banking expertise to review the bank’s compliance audit to ascertain whether the employees have breached the implied or express terms of their employment contract or bypassed any risk and AML regulations, investigated suspected fraud or circumvented control by the employee, or failure of management to perform their duties, investigated constructive fraud based on a breach of an alleged fiduciary duty or breach of confidence, investigate the context in which the type of alleged fraud took place and whistleblowers' complaints, question the reporting lines and why the IT system was "standalone" and separate from the corporation's system.

In a merger and acquisition transaction such as Sampo Bank, an FA could have analyzed the future growth prospects of the target company, including comparing cash projections of the competitors, provided research and investigation techniques into the company's background,

including conducting background checks on key employees and clients, both resident and non-resident, and for politically exposed persons.

The Financial Action Task Force defines clients and politically exposed persons who have been entrusted with a public office or function and may be vulnerable to financial crimes such as corruption and money laundering. The FA can uncover relevant documents, review and document the lack of complete or accurate documents, inform the parent company of breaches in regulations and crucial facts about the target company which could affect the purchase and/or purchase price.

In the course of performing a forensic accounting engagement, an IFA practitioner can identify the alleged fraud data and fictitious in the case for potential litigation: by analyzing overstated revenues and/or understated expenses through horizontal and vertical analysis, management and executive inefficiencies in following regulations, laws, industry methods, business process deficiencies in comparison to competitors or industry norms for those following legislation and regulations.

4. 4 Analysis of Wells Fargo Bank Systemic and Corporate Failure

The Justice Department and Securities and Exchange Commission struck a three-year deferred prosecution agreement with the nation's fourth-largest bank. Wells Fargo admitted it collected millions of dollars in fees and interest that it should not have collected, harmed the credit ratings of customers, and unlawfully misused customers' sensitive personal information. Wells Fargo's $3 billion fine includes a $500 million civil penalty to be distributed by the SEC to investors. The Office of the Comptroller of the Currency said that former Wells Fargo CEO John Stumpf, has been barred from working at a bank again and will pay $17.5 million for his role. Reuters on March 1, 2019 reported that Wells Fargo's was fined $240 million US, as executives and directors breached their fiduciary duties by disregarding the complaints of bogus accounts and failing to stop their creation in September 2016. (See appendix 7)

Reasons for risk management failure

1. Senior management and the board of directors failed to provide insight into ERM's role in setting the strategy or setting the tone at the top in support of the risk management framework and model.
2. Senior management failed to assess the range of outcomes that might occur, as indicated by the lack of oversight, monitoring, managing risks.
3. Senior management and the board were not experts or trained. As a result, they were Risk ignorance and miss-measured the known risks. They did not have the appropriate expertise on risk and risk mitigation and failed to seek external third parties to provide effective oversight of banking risks.
4. There was Agency risk, where middle managers and employees wittingly or unwittingly do not succeed in pursuing procedures intended to manage and moderate risks, and there was no focus on continuous improvement as applied to the enterprise risk management process itself.
5. Shifts or changes in the threat landscape are inherent in the form of new and evolving risks. Organizations may moderate risk by either acquiring insurance, reducing it, transferring it, or avoiding it altogether. However, these proceedings did not address or eradicate the systemic risk
6. Incremental enterprise risk management failure is frequently caused by an extensive incubation period from the degradation of the risk management processes over a long time
7. Failure to regularly, objectively, and fairly report risks to the Board and the top management: Once risks are identified and quantified, they must be actioned at the organizational upper management level. The inability to properly communicate risks to senior management may cause overall risk management failure. These failures are an indicator of unnecessary risk acceptance and or exposure In the Risk management failure literature
8. Failure to use appropriate risk metrics or measurement system. Risk management failure can be caused by the use of improper risk metrics, which induces inaccurate measurements. The most common risk metrics in modern risk management is "Value at Risk" (VaR). Although VaR has been proven to be a quintessential risk measure, meaningfulness is directly dependent on the quality of the associated answer and original question.

4.5 How Can A FA Help Wells Fargo Overcome Systemic and Corporate Failures?

ERM's main objective is to improve the corporation's understanding of the impact of risk arising from culture, strategy, and performance. Given the number of code of conduct breaches, cyber breaches, exposed cloud storage units, ransom ware attacks, and other adverse cyber-related events that continue to rattle the banking industry, applying the benefits of an appropriate ERM should be a top issue for Boards and the C-suite. Here are some key principles objectives based on the COSO 2017:

- Define the desired corporate culture, develop a code of conduct, link the strategy to performance, and risk management. Management should set objectives, identify the risks and opportunities that align and support the entity's mission, define its risk appetite, identify the risks inherent in the business model, evaluate and assess risk mitigation techniques, which is essential to avoid such failures.
- Top management must have the talent and expertise to hold positions of fiduciary trust; the culture should also support the careful selection of skilled and trained employees who can recognize and report activities that make the organization vulnerable to considerable or significant risk.
- Establishing responsibility through policies and procedures for reporting on risk, culture, and performance, building procedures for the timely escalations in addition to building a common risk language, shared definitions, a shared culture of risk awareness and clearly understood procedures for measuring, monitoring, communicating and dealing with risks are very imperative for mature Risk Management approach.
- Communicate upstream and downstream regularly on risks that are dynamic and more complex to measure and for which results cannot be easily forecasted with minimal confidence. The organization should have a budget for external expertise to consult on minimizing disruptions based on the risk appetite for unacceptable risk exposures.
- Organizations should consistently manage risks by monitoring and continuously seeking opportunities to improve their risk stance. If an organization must achieve these, concrete plans should be enforced top-down balancing 1) risk and benefit and 2) risk and cost. Monitoring, evaluating activities, and making modifications are accomplished through ongoing management activities, separate evaluations, or both.

To elaborate on how to overcome risk management failures within banking industry, let's examine the systemic and corporate failure at Wells Fargo Bank and the credit cards stolen case depicted below as an illustrative example. This will further support the argument and premise of this paper about how a "Forensic Accountant" can add competitive advantage to risk management functions of a bank.

An overview of conduct risk and corporate failure at Wells Fargo

1. Prolonged sales practice violations that included opening over three million unauthorized deposit and credit card accounts between 2011 and 2016 undetected
2. Rationalization- The CEO and the senior executives downplayed the severity of the situation. They tried to justify that the terminated employees represented only 1% of the bank's workforce and framed the problem as a few bad apples—failure to investigate and appropriately respond to whistleblower reports adequately.
3. Unethical corporate culture, lack of management oversight and failure to meet and comply with supervisory expectations
4. Inability to execute, implement and monitor effective corporate governance and an appropriate risk management program
5. Tone at the top - evidence of rationalization, failure to understand the risk appetite, inability to manage conduct risk and aggressive culture on the part of the senior executives and managers in the Wells Fargo's sales scandal. According to the Los Angeles Times, "employees were much more likely to be disciplined for failing to meet their sales targets.....than for engaging in sales practices misconduct."
6. Corporate governance failure- Evidence of compliance disaster, culminating in dysfunctional corporate board governance and oversight of senior management and corporate operations.
7. The sales incentive program designed and implemented by Wells Fargo was built on incentivising sales and punishes those who do not meet the objectives. This is fundamentally called into question the board of directors' commitment to its fiduciary trust.

According to the Ethical boardroom, "The Federal Reserve's consent order required Wells Fargo to submit three separate written plans." The first is to improve its board of directors' effectiveness. The second is to strengthen its firm-wide compliance and operational risk management program. The third requires Wells Fargo to conduct and complete by September 30, 2018, an independent review of its board's improvements ineffective oversight and governance and enhancements to its compliance and operational risk management program.
"My question is why regulatory bodies wait until after the Wells Fargo fraudulent sales practices scandal hits the news to put such measures in place, especially after the lessons learned from 2008 financial scandals?"

Following the integration of the improvements required by the order, Wells Fargo was required to conduct a second independent review to assess the efficacy and sustainability of the improvements. Forensic accountant would have helped Wells Fargo design and implement an effective internal control framework to enhance the board of directors' effectiveness by performing followings:

- Ensure the bank's strategy, and risk tolerance are aligned with the bank's risk management capacity
- Ensure the board's composition, governance structure and practices support its strategy and are aligned with its risk tolerance
- Ensure the board's roles and responsibilities do not go unfilled for an undue period following the departure of any board member
- Improve the board’s oversight of senior management
- Ensure senior management’s ongoing effectiveness in managing the bank’s activities and related risks
- Ensure that senior management establishes and maintains: (i) an active and independent firm-wide risk management function; (ii) an effective —risk tolerance program; (iii) a sufficient risk identification and escalation framework; (iv) a comprehensive and effective risk data governance and management framework

- Ensure that compensation and incentives reinforce and are relevant to risk management objectives and measurement standards, including consequences for violation of its policies, laws and regulations and adverse risk outcomes
- Ensure that comprehensive reporting will enable the board to oversee management's execution of its risk management responsibilities, including measures taken to comply with the consent and provide the board with sufficient information to evaluate the operational and compliance risk management functions.

4.6 Case Study: Stolen Credit Cards and Involvement of Forensic Accountant

- The bank was losing millions of dollars to fraudulent purchases made using stolen credit cards. The audit director had been asked to find a way to identify inappropriate purchases as early as possible, even if the card had not yet been reported as stolen. During a brainstorming session with the forensic auditors, regression analysis and two other tests were suggested.
- Regression analysis performed by a forensic accountant was used to compare each transaction for each cardholder to their typical purchasing pattern. Anomalies were identified, and cardholders were called to determine if they had made the purchase. The results were terrific. After several months of refining the program, transactions were being selected in many cases where the cards had been stolen; detecting the fraud after only a few purchases had been made.
- The second analysis involved reviewing transactions by vendor. Vendors who were not frequently used, or part of the customer's purchasing pattern were flagged as result of forensic accountant expertise in use and analysis of big data, and the cardholder was called to verify the purchase.
- The third analysis performed by a forensic accountant was a comparison of the date and locations of the purchase. Two purchases made on the same day, but in widely separated zip codes, would cause a flag to be set. The rationale was that it was unlikely that two purchases would be made in different parts of the country on the same day, so verification was obtained from the cardholder. Finally, an analysis was performed to identify even amounts and purchases from the same vendor on the same day. While these

sometimes erroneously flagged transactions as potential frauds, the value of the fraud prevented substantially outweighed the administrative costs of checking with the cardholders based on an FA cohort analysis. Also, many cardholders were pleased that the company had taken a proactive approach to prevent stolen credit cards—a valuable, intangible benefit.

Scheme: Theft of credit cards

Symptoms: Unusual patterns in the data (same vendor same day, even amounts, split purchases, abnormal amounts); unusual vendors

Data Requirements: Credit card—card number, date, amount, merchant, merchant address

SECTION 5

HOW CAN A FORENSIC ACCOUNTANT ADD SUSTAINABLE VALUE TO ENTERPRISE RISK MANAGEMENT?

Risk is inherently embedded into any business activity, process, system and program. According to M. Mendes da Cruz and Sonia R. Bentes who asserted that technological and economic developments have brought new dimensions to business risks and sometimes producing effects that are difficult to control. According to ACFE, forensic accountants combine their accounting knowledge with investigative skills, using this unique combination in litigation support and investigative accounting settings. Forensic accountants may be employed by public accounting firms' forensic accounting divisions, by firms specializing in risk consulting and forensic accounting services, or by lawyers, law enforcement agencies, insurance companies, government organizations, or financial institutions. Due to society's heightened awareness and growing intolerance of fraudulent activity, resulting in financial loss, ruin and reputation the demand for forensic accountants is rapidly increasing. Consequently, followings are identified as critical functions of forensic auditor and investigation[16]:

[16] The Effectiveness of Forensic Auditing in Detecting, Investigating and Preventing Bank Frauds: Journal of Sustainable Development in Africa (Vol. 10, No.4, 2009)

1) To carry out the vision and mission of forensic audit to prevent, detect, and investigate fraud and financial abuse issues within an organization or entity
2) Identification of causative factors and collection of facts for individual investigations by leading the evaluation of internal control weaknesses allows unethical business behavior and practices to occur and go undetected
3) Lead internal/external resources to address allegations of fraud raised within the system
4) Provision of help in the development of fraud awareness training and analyze fraud trends and internal control procedures
5) Perform a comprehensive analysis of investigations result across the enterprise to identify pervasive control issues
6) Oversee the investigations, planning, and forensic report writing processes for forensic audits, as well as investigations and presentation of findings through reports and exhibits
7) Work closely with financial training function to enhance fraud-auditing skills
8) Develop the fraud prevention, detection and investigation programs, and management of the company's fraud risk assessment and profile programs
9) Conduct complex and compassionate investigation
10) Conduct activities in areas of moderate to high risk
11) Promote education and awareness about fraud risk management throughout the bank
12) Testifying in court as an expert witness where and when necessary.

There is no doubt that "qualified, trained and mature accounting professionals, possessing forensic skills, can prove to be a valuable asset to the corporate-sector, and gradually help to improve their corporate governance (CG) and risk management functions." FAs are in great demand for their accounting, auditing, legal, and investigative skills. They can play a vital role in coordinating company efforts to achieve a cohesive policy of ethical behavior within an organization. FA's are expected to be a specialist in accounting and financial systems. Yet, as companies continue to grow in size and complexity, uncovering fraud requires FA's to become proficient in an ever-increasing number of professional core skills and competencies. Below are

some of the broad areas of useful expertise for FA's according to international journal of contemporary business studies:

1) In-depth knowledge of financial statements and the ability to critically analyze them. These skills help forensic accountants to uncover abnormal patterns in accounting information and recognize their source.
2) A thorough understanding of fraud schemes, including but not limited to asset misappropriations, money laundering, bribery and corruption
3) The ability to comprehend the internal control systems of corporations, and to set up a control system that assesses risks, achieves management objectives, inform employees of their control responsibilities, and monitors the quality of the program so that corrections and changes can be made
4) Proficiency in computer and knowledge of network systems. These skills help forensic accountants to conduct investigations in the area of e-banking and computerized accounting systems
5) Knowledge of psychology to understand the impulses behind criminal behavior and to set up fraud prevention programs that motivate and encourage employees
6) Thorough knowledge of the company's governance policies and the laws that regulate these policies
7) Command of criminal and civil law, as well as, of the legal system and court procedures

Forensic accountants can add competitive and sustainable value to an organization's risk management functions in these following ways:

1) Corporate Governance: With a strong background knowledge of the legal and institutional requirements of an organization, a forensic accountant can help formulates and establish a comprehensive corporate governance policy that; 1) ensures an appropriate mix of the management and independent directors on the board, 2) set out the appropriate responsibilities of the board and 3) ensures there is a company code of ethics for employees and management. Ethical behavior is reinforced when top management shows that questionable behavior will not be tolerated through its actions.

2) Preventing Fraud: Involvement of a forensic accountant in the risk management board and at the early stage of systems promulgation is the best way to detect and prevent fraud at the early stage. This is partly because FAs understands that the best way to avoid fraud is to establish an effective and efficient internal control system that encompasses: a right control environment determined by management's philosophy of ethical behavior and strong corporate governance (CG) policies; a superior accounting system that ensures the proper recording, classification, and reporting of all relevant transactions; and strong procedural controls that provide for the safeguarding of assets, proper authorizations, audit mechanisms, and proper documentation

3) Establishing Effective Lines of Communication: According to Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Effective communication must flow from the top to lower levels, but also across employee lines of responsibility." Forensic accountants can, by virtue of their vast knowledge and experience in adequate reporting necessary to meet the compliance requirements, help to establish and disseminate accurate information about ethics and robust corporate governance policies.

4) Vigilant Oversight: For any system to function well and achieve its intended purposes, there has to be constant monitoring and evaluation procedures in place. Forensic accountant can help banks to realign its governance, ethics, and internal control policies by effective monitoring of not only compliance, but also risk management procedures and employees activities embedded in risk management functions.

5) Establishing Consequences: Forensic accountant can help organization in creating policies that clearly state the company's intent to take punitive action against any criminal activities. This is possible because of an FA's knowledge of psychology to understand the impulses criminal behavior and to set up fraud prevention programs that change employee’s orientation towards fraud.

6) Fraud Investigation: Forensic accountant techniques in combating corporate crime by providing accounting analysis, scope of expertise, rules of evidence suitable in court of law for the purpose of admissibility. Although forensic auditors does not determine the existence of fraud. However, forensic investigative procedures attempt to uncover irregularities that indicate the presence of assets misappropriation or fraud activities.

5.1 Differentiating factors between Forensic Accountants (FA) and other Professionals.

In section (3) above, skills required of risk management expert, traditional accountant and forensic accountant relative to risk management functions was enumerated and explained. However, forensic accounting peculiar skills have become crucial in untangling the complicated accounting and risk management manipulation that have obfuscated financial reporting due to lack of oversight in risk management functions within financial institutions. According to journal of accounting-business management, "financial community realized that there is great need for skilled professionals that can identify, expose, and prevent structural weaknesses in three key areas: poor corporate governance (CG), flawed internal controls, and fraudulent financial statements." The journal therefore asserted that "Forensic accounting skills are becoming increasingly relied upon within a corporate reporting system that emphasizes its accountability and responsibility to stakeholders." (JABM Volume 20 (2) 2013).

Followings are in exhaustive list of the forensic accounting skills that differentiate forensic accountant from other professionals or how an FA can add competitive advantage to risk management functions within financial institutions:

Preservation, mitigation, and stabilization of data:

It's imperative to consider steps necessary to safeguard and to stop further loss of data, funds, and other assets when trying to mitigate risk. These might include the closing of bank accounts, freezing of emails and other communication channels, deactivating user passwords, and other necessary steps to deny access to investigation subjects. Forensic accountants leverage and provide their investigative and auditing skills to preserve and stabilize financial and accounting documents depending on the nature of the investigation through the following list of activities. This capability makes forensic accountant to stand out among other professionals in adding value to risk management functions.

Determining the violation of internal controls:

It is essential to establish whether the act was intentional before an investigation procedure. However, intent could be complicated to prove in a court of law by anyone. Notwithstanding, demonstrating that a subject violated a documented, well-established internal control could

corroborate the fact. Determining how an internal control was circumvented or otherwise violated could also explain how fraud or corruption was perpetrated because establishing that a subject intentionally violates internal controls can be essential to support the argument for criminal prosecution or regulatory enforcement process. Such understanding is also very critical to developing a remediation plan to shore up controls to prevent future occurrences.

Forensic data analysis

Forensic accountant/investigator expertise in data analytics and data mining can help in an investigation process to analyze electronically stored financial and accounting data. Analysis of non-financial data is also within the purview of forensic accountant skills. Data analysis is relevant to forensic accounting knowledge and helps the investigative process as follows:

1. to initially detect fraud or non-compliance
2. to corroborate an allegation to justify launching an investigation, prove merit over substance (e.g., proving that an allegation received via a hotline appears to have merit); and
3. to perform certain parts of the investigation

However, data analytics rarely prove that fraud or non-compliance occurred. Instead, data analysis identifies transactions or activities with the characteristics of fraud or non-compliance known as anomalies, so that they can be examined further. Further analysis of additional facts makes the distinction between an intentional act of fraud and an escalating series of honest mistakes and helps the investigation.

Regression/Trend Analysis:

Forensic Accountant performed regression/trend analysis that allows them to graph a wide variety of linear and nonlinear relationships to detect anomalies. The advantage of regression analysis lies in the ability to estimate values even when the relationship is not linear and, therefore, not intuitively obvious.

Data mining to detect fraud or sharing of information:

Analysis of statistical data by a forensic accountant/investigator makes it possible to detect an unusual number of high-acclaimed frauds and/or claims. Although, data analysis does have its limitations, such as fraudulent claims or acclaimed frauds, not meeting pre-defined search

criteria and likely to slip through the cracks and go undetected. However, with forensic accountant special skills and understanding of data mining, organizations can at least potentially address this problem by refining the detection rules, increase effectiveness and analyze the practice profiles17. Daniel Tourangeau (2017) further alluded that advanced data mining has enabled organizations to considerably reduce the amount of time invested in trying to detect fraudulent claims and acclaimed fraud cases.

Corroborating allegations:

This is significantly advantageous and sets a forensic accountant apart from their accountant counterparts and risk management officers. This is because a forensic accountant can perform these on electronic data without even alerting the subject of the investigation and or during an interview process of any alleged fraud cases. Nevertheless, a forensic accountant will first assess the allegation in terms of what impact the alleged fraudulent or corrupt act will have on financial and/or non-financial data and the validity of such allegations. A comparison of anomalies with data from similar transactions that do not involve fraud or non-compliance is another source of corroborating allegations by forensic accountants that can invariably add sustainable value to a bank's risk management functions.

Use of Artificial Intelligence:

A forensic accountant has introduced the use of AI as an alternative to the old sampling methodology used by traditional auditors. This allows for the analysis of thousands of transactions over multiple fiscal years within a significantly reduced timeline. The utilization of these AI platforms dramatically improves the efficiency of forensic audits and reduces the timeline of work performed. Artificial Intelligence (AI) has emerged as a useful tool in dissecting financial data over multiple years to identify spending patterns and high-risk transactions[18].

Using data analysis in an investigation:

The final application of forensic data analysis is in the inquiry itself, which is also within the domain and expertise of the forensic accountant. Once an allegation has been substantiated, or a

[17] Data mining and information sharing: two essential tools to stop insurance fraud and abuse. Daniel Tourangeau|LBC Meaden & Moore International (2017)

[18] Association of Certified Fraud Examiners (ACFE) 2018

first anomaly has been found to involve fraud or non-compliance, forensic account/investigator may perform additional forensic data analysis to:

1. determine how long the activity has been going on;
2. determine which employees (or third parties) have played roles (i.e., assessing whether collusion was involved);
3. measure the financial damage resulting from the activity; and
4. identify other fraudulent or corrupt conduct by the same individuals.

Determining who is involved in fraud or fraudulent act has become increasingly important over the years, according to a recent report by the Association of Certified Fraud Examiners (ACFE).

e-Discovery and litigation holds

It is within the purview of IFAs knowledge and skills to identify and preserve any relevant data that might be useful in an investigation (e-Discovery) and to communicate any litigation hold to all pertinent individuals and/or departments to avoid accidental destruction of critical evidence or records. Owing to the proliferation of electronic data, it has become increasingly crucial for a forensic accountant to determine, before any investigation, what relevant information exists and in what format (paper or electronic); where it is located or stored (on-site database, off-site vendor, or in the cloud); what security measures in place to protect the data; and what is the organization's standard policy and procedures on record retention and destruction

Review of supporting documents

This is a judgmental call to testing for the authenticity of the record or of individual signatures on documents that generally involve a highly specialized skill that ultimately possessed by a forensic accountant. Accordingly, if an IFA suspects that a document on file is fraudulent or has been physically altered or that a signature is not authentic, such a document would be protected until someone with the specialized skills necessary to assess authenticity is called on.

Studying and understanding the processes and internal controls involved in the transaction cycle suspected in the investigation should result in a list of relevant documents. For example, in a procurement transaction, several paper documents may need to be reviewed:

- budget authorization form and approval
- request for tender to approved vendors
- bidding documents received from bidders and reviewed
- contract terms and service level agreements
- purchase order or purchase request approval
- bill of lading or other confirmation of delivery of goods
- signed confirmation for services provided
- invoice from a vendor or supplier; and
- cheque or disbursement request form.

Some of the most common reason these documents would be reviewed include:

- establishing a timeline and a trend of events
- testing clerical accuracy
- reviewing for inconsistencies (e.g., a price reflected on a purchase order that was inflated on the final invoice)
- reviewing for agreement with accounting records; and
- reviewing for compliance with internal controls.

Tracing assets

Another key differentiator factor where a forensic accountant can add value to risk management function is the tracing of assets. FAs' acquired a degree of knowledge and skills to develop a recovery plan and implementation of remedial measures to ensure that similar losses don't arise in the future. A successful asset recovery strategy combines creativity, investigative cunning, and litigating skills. FA can also detect any public trail of valuable clues regarding the disposition or location of illegally obtained funds and assets.

SECTION 6

HOW A FORENSIC ACCOUNTANT CAN ADD VALUE TO THE FUTURE OF ENTERPRISE RISK MANAGEMENT FUNCTIONS AT BANKS

Risk management functions have continued to evolve and update over the years across financial institutions and large corporations with global digital initiatives, customer demands, changes in regulations and the fines levied for non-compliance of these regimes. CEOs and CFOs have triggered a wave for change in risk management functions such as BCBS 239[19]. The management of non-financial risk will also be measured and monitored as industry standards are compared, compliance and conduct is enforced, stress testing is reviewed by management and decisioned concurrently with the range for risk-appetites; banks will also invest in identifying their risk cultures, closely involve qualified boards and experts who will guide with critical risk decisions. Finally, as banks strive to define, delineate and monitor their lines of defence, the magnitude of these shifts will require risk functions in banks to transform using tests, technology such as artificial intelligence, academics and forensic accountants to meet these increased demands.

It is inevitable that banks' risk functions will continue to experience more stringent regulatory reporting, financial crises, technological disruptions to risk management, cyber currency impacts and black swan effects, all of which are likely to reshape banks and their risk management regimes.

1. Continued expansion of the breadth and depth of regulation

According to McKinsey's working paper on risk, Supervisory oversight practices should evolve as the scope of regulation continues to expand. Government tolerance for bank failures has shrunk; government policing of illegal and unethical behavior; government increasingly demanding both domestic and global compliance (extraterritorial) with their regulatory standards etc. Consequently, shortly, banks will probably have to provide more stringent supervisory

[19] McKinsey working papers on Risk

oversight with even more information and support their claims with quantitative data. This will be in the form of a Comprehensive Capital Analysis Review (CCAR), as requested in the United States, and a survey that tracks progress and benchmark the Canadian banks against its peers. These regulatory trends are expected to have substantial implications for banks' risk management, by demanding for highly analytical business optimization and strategy-setting process[20]. A forensic accountant could play a key role because of their expertise and superior skills in all these areas.

2. Changing customer expectations

Over the next decade, shifts in customer expectations and technology are expected to cause a significant paradigm shift in the banking sector and create an entirely new different profile[21]. By then, widespread proliferation and the use of technology is likely to be the norm for customers. Over the last two years, the amount of innovation has increased across the sector, and investment in financial-technology (fin-tech) start-ups has grown exponentially. Innovation affects every part of the value chain, but an essential disruption will probably occur in banks' origination and sales processes as reiterated in McKinsey's working paper on risk. Therefore, to deliver on the customers' expectations, banks will probably require redesigning the whole organization from a customer-experience perspective and digitizing at scale.

However, to achieve this, the risk function will need to be a core contributor and collaborate closely with the overall business strategies. It would most likely focus on two priorities as depicted in the journal, the future of bank risk management[22]:

a) Banks will have to offer rapid real-time answers to customer requests with highly customized processes (Automated instance decisions);
b) Tracking activities and preferences of a single potential customer, then tailoring products for that individual according to their behaviors ("segment of one"). However, to achieve this;

[20] McKinsey Working Paper on Risk
[21] McKinsey Working Paper on Risk
[22] McKinsey Working Paper on Risk

i. risk functions will likely need to find ways to help banks assess risks and make decisions without human intervention, which often calls for zero-based process redesign and use of more non-traditional data[23]; and
ii. risk functions will be expected to work with operations and other functions to find ways to manage these emerging concerns while still providing highly customized solutions[24].

Therefore, a forensic accountant with the proliferation of artificial intelligence (AI) and big data can help banks to aggregate customers' interactions across multiple touch points, which should – in theory – mean that bank understands their customers' behaviour, preferences and expectations better than ever before.

3. Technological and analytics as a risk muscle

Technology will change customer behavior and enable new risk-management techniques, often coupled with advanced analytics. The proliferation of new technologies provides cheaper, faster computing power and data storage, which will allow better risk decision support and process integration. Currently, banks are experiencing the effects of some innovations such as big data, machine learning, and crowdsourcing that have tremendously improved risk management function.

Involvement of a forensic accountant in risk management functions of a bank with a proliferation of advanced computer skills enumerated will add value to a bank's risk management as follows:

i. Significantly improve the predictive power over time, data protection and preserve evidence in a way that is acceptable to the court;
ii. Validation of external and unstructured data for a more substantial upside for better risk analysis, early warning (Red flags) and effective portfolio monitoring; and
iii. Much deeper insight into data, identification of complex, nonlinear patterns in large data sets, and provision of more accurate risk models for accurate and seemingly decision making.

4. Additional (non-financial) risk types are emerging

[23] McKinsey Working Paper on Risk
[24] McKinsey Working Paper on Risk

The tremendous increase in fines, damages, and legal costs related to operational and compliance risk has forced banks to pay more attention to these risks over the past five years. This will probably increase even further, due to the regulatory trends and given the expected rise in capital requirements for operational risk[25]. Examples of such emerging non-financial risks include:

i. Contagion risk
ii. Model risk
iii. Cyber attacks

A forensic accountant can significantly help the bank to reduce overall total risks by minimizing these risks and lower its capital requirements and surcharges. Thus, add competitive and sustainable value to risk management function as follows[26]:

a. to continually measure, monitor and track these risks;
b. use and understanding of big data, artificial intelligence (AI) and data normalization to help increase data quality, detect any technical or implementation errors, correlation or time inconsistencies, and any uncertainties about volatility; and
c. development and adoption of rigorous sophisticated and multiple mitigation strategies for better execution, proper data validation, and constant monitoring and improvement of risk models.

5. Better risk decisions through the elimination of biases

Hindsight and cognitive biases are simply put, systematic errors in thought that can emerge at every stage of the risk assessment process, thus producing skewed and unreliable results that can directly impact decision making.

Consequences of hindsight bias, for instance, include myopic attention to a single causal understanding of the past (to the neglect of other reasonable explanations) as well as general overconfidence in the certainty of one's judgments[27]. However, it is not only the informational content that matters for hindsight bias or cognitive bias but also the subjective ease with which that informational content is processed as alluded to in McKinsey's working paper on risk.

[25] McKinsey Paper on Risk
[26] MFAcc IFA 2905 Material (2017)
[27] Hindsight Bias APS 2012

Because FAs err on the side of caution when it comes to the issue of risk compliance and legal ramifications, it's therefore easy for them to understand cognitive bias and implement strategies and best practices to mitigate any effects that bias may have on the organization's overall risk assessment. Determination of the circumstances whether expert evidence is admissible in court or not, is also another extenuating factor when dealing with litigation associated with bias case in court.

i. **Use multiple points of view or mapping algorithms**[28]: FAs view different visualizations at the same time, to prevent a single, arbitrary angle from dominating interpretation leveraging on data mapping and "The consider-the different de-biasing strategy to avoid bias and single interpretation based on visual perspective.

ii. **Balancing out the sample selection**[29]: The forensic accountant uses simulated experiments in which some parts of a database are removed as the basis of the visualization. This will enable FAs to determine how much does the visualization change or see if the change support, or contradict the current interpretation. This invariably will result in reducing or eliminating selective bias or misattribution of processing fluency to overconfidence that can impair risk management decision-making.

iii. **Balancing out the sample solution**[30]: FAs ensure that sample selection contains variables with balanced perspectives and varied incentives to avoid sample bias. Broader and more focused sample selection help offset biases that might exist

iv. **Using data to combat fundamental biases**[31]: FA's objectivity and valid measures to quantifying risk help to minimize biases and limit the impact of such biases (availability and anchoring biases). This will definitely help align reactionary thinking with analytical reasoning[32]and ultimately enhance risk management functions and aid risk decision making processes

[28] Corporate Compliance Insight (2019)
[29] Corporate Compliance Insight (2019)
[30] Corporate Compliance Insight (2019)
[31] Corporate Compliance Insight (2019)
[32] Corporate Compliance Insight (2019)

SECTION 7

CONCLUSION

Risk and fraud prevention is one of the most critical aspects of an effective organizational risk management strategy. According to the Association of Certified Fraud Examiners (ACFE), there were 2,690 cases of occupational fraud, resulting in over $7 billion in total losses over 125 countries and 23 industry categories. Almost half of all fraud cases resulting from weaknesses in internal controls and 11% of fraud cases involving executives/upper management ensure that adequate internal controls are in place is critical to preventing fraud. To protect and respond to fraud, many organizations have turned to forensic accounting and the use of artificial intelligence (AI) as part of their risk management strategy[33].

In general, Risk management is the process of identifying, evaluating, selecting, and implementing actions to reduce risk. The goal of risk management is to develop a shared understanding of risk across multiple functions and business units to manage risk cost-effectively on an enterprise-wide basis, integrated actions that reduce or prevent risks while taking into account social, cultural, ethical, political and legal considerations. The FCAC stressed that bank boards were failing to effectively manage risks "inherent" to their institutions' profit-driven cultures, in part because they lacked a "consolidated and holistic view" of sales-practice risks. FCAC further alluded that, 1) "Board, senior management, and control functions are limited in their ability to identify, measure, monitor, and address risks related to misspelling, poor consumer outcomes, and breaches of market conduct obligations." 2) "Governance frameworks and control mechanisms do not effectively manage or mitigate the risks inherent to cultures that are so heavily anchored in sales."

A forensic accountant under contemporary conditions is undoubtedly essential because it will significantly enhance banks' risk management functions in those areas highlighted by FCAC.

Also, increasing occurrence of fraud risk in the modern-day business environment and continued traditional audit failures over the past decades have prompted a paradigm shift in accounting and

[33] Association of Certified Fraud Examiners (ACFE) 2018

should prompt the same paradigm shift in risk management functions within banks. Therefore, various agencies fighting corruption and managing risks worldwide will have to engage the forensic accounting service to complement other professionals' efforts in installing fraud-risk-proof internal control systems, enhancing risk management functions to add competitive and sustainable values to overall risk management functions of a bank.

SECTION 8

RECOMMENDATIONS:

Despite the newly revised laws and regulations, fines, and penalties levied against financial institutions and other large organizations to mitigate the risk of financial frauds, there are still breaches. Why? This is mainly due to management and senior executives' lack of oversight over resources for expertise, redesigned systems, training of staff and anticipating the emerging risks. The following areas need to be critically looked into as a forensic accountant to add a competitive advantage to the bank's risk management functions:

1. ***Avoid Function Trap***: Banks should avoid the cognitive-behavioral trap by not compartmentalizing their risks but rather approaching them holistically
2. ***Effective Management of Uncontrollable Risks:*** Most external risks lie primarily outside the institution's control and can't typically be reduced and/or avoided through the same approaches used for managing preventable and strategic risks. Therefore, banks need to focus on identifying these risks, assessing their potential impact, and see how best to mitigate their effects even before they occur
3. ***Involvement of FA in a Risk Assessment and Mitigation Committee:*** Bank's risk profile can change dramatically based on a decision made inappropriately. Consequently, risk management requires embedded experts within the institution to monitor and influence the risk profile continuously. Therefore, the involvement of a forensic accountant in such a committee, working together with other line managers in formulating risk management policies and procedures will add a competitive advantage to the whole process
4. ***Strengthen Oversight by Branch Managers:*** According to FCAC, branch managers have “limited line of sight” into customer interactions and are unlikely to have sufficient resources to execute proper oversight. Therefore, banks can improve branch managers’

oversight by increasing their investment in data gathering and analysis tools. Which of course, is part of the skills and expertise of a forensic accountant

5. ***Apply Data Analytics to Customer Complaints*:** Recording and analyzing all customer complaints would significantly increase a bank's ability to monitor, identify, and correct problematic risk-related sales practice trends. Frontline staffs resolve most customers' complaints, and they are not logged into a central database due to inadequate skills and knowledge about fraud risk-related policies and procedures. Incidences like this should be within the purview of a forensic accountant because of their expertise in data analytics and adequate documentation;
6. ***Increase Investigation of Root Causes***: To reinforce data analytics and pattern detection, banks should investigate the root cause of customer complaints. For example, if a customer complains about a surprise fee, banks should not merely reverse the fee and record a closed case. Further investigation may uncover breaches of disclosure and consent-acquisition obligations, which may indicate a need for re-training or discipline. The FCAC found numerous instances of inadequate complaint investigations, with banks limiting their inquiries to the extent needed for a quick resolution, making "little effort to identify root causes";
7. ***Environmental and Social Risk Management Policies**:* FAs should help banks to proactively review and update its ESRM policies and procedures to address regulatory changes, emerging and evolving issues, internal best practices and most importantly to consider the impact of environmental and social issues on all its activities;
8. ***Development of Risk Categories**:* FAs can help in the development of risk categories that will define the types of fraud risk an organization may be exposed. Typical risk categories include the external environment, legal, regulatory, governance, strategy, operational, information, human resources, financial and technology[34].
9. ***Reviewing and Investigating Systematic Risk Fundamentals*[35]**: The Forensic accountant's involvement in the area of systematic risks identification is helpful and highly recommended. For example, the CBC news of January 28, 2013 reported that David Beattie of Moody's, stated that the high levels of consumer indebtedness and

[34] Computer-Aided Fraud Prevention and Detection (Chapter 2). MFAcc 2017 material
[35] The CAPCO Institute Journal of Financial Transformation(2015)

elevated housing prices leave Canadian banks more vulnerable than in the past, to downside risks the Canadian economy faces. Therefore, involvement of forensic accountant in reviewing and investigating systematic risk will ultimately help lowering the risk of consumer indebtedness and investigating the causal effects of elevated housing prices will ultimately enhance banks' overall ERM and add competitive advantage.

9.0 Interview Questions

Question for DIFA-MFAcc Graduates working in the Banking Sector

Do you think that a graduate of the DIFA or MFAcc programs could offer significant additional value in risk management services in Canadian banks compared to other forensic accountants? Please consider the following risk management aspects and identify the aspects, if any, in which you foresee significant additional value:

- Strategy
    - Determination of appetite for risk taking.
    - Determination of risk management strategies.
    - Determination of clear risk categories.
    - Determination of innovative opportunities.
    - Recognition that underlying risk assumptions are too optimistic, pessimistic or invalid and how?
    - Early recognition of the need for strategies and procedures to discover and manage risks for Back Swan, systemic developments (i.e. COVID).
- Culture
    - Detection of weaknesses in risk management culture.
    - Recognition of when strategy and culture are misaligned.
- Procedures
    - Timely adaptability of risk management procedures.
    - Recognition of when further analysis or clarification is required.
- Skills
    - Identification of risks.
    - Detection of new potential risks.
    - Development of new skills for emerging areas of risk.

10.0 Appendices

Appendix 1 Drivers of Misconduct, Restoring trust and Conduct Risk

(Source: Deloitte Center for Regulatory Strategy)

Responses for restoring trust

(Source: Deloitte Center for Regulatory Strategy)

Innovative solutions for managing conduct risk

(Source: Deloitte Center for Regulatory Strategy)

Appendix 2: The FATF 40 Recommendations on AML/TF (2012-2019)

THE FATF RECOMMENDATIONS

INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION

THE FATF RECOMMENDATIONS

Number	Old Number[1]	
		A – AML/CFT POLICIES AND COORDINATION
1	-	Assessing risks & applying a risk-based approach *
2	R.31	National cooperation and coordination
		B – MONEY LAUNDERING AND CONFISCATION
3	R.1 & R.2	Money laundering offence *
4	R.3	Confiscation and provisional measures *
		C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION
5	SRII	Terrorist financing offence *
6	SRIII	Targeted financial sanctions related to terrorism & terrorist financing *
7		Targeted financial sanctions related to proliferation *
8	SRVIII	Non-profit organisations *
		D – PREVENTIVE MEASURES
9	R.4	Financial institution secrecy laws
		Customer due diligence and record keeping
10	R.5	Customer due diligence *

11	R.10	Record keeping
		Additional measures for specific customers and activities
12	R.6	Politically exposed persons *
13	R.7	Correspondent banking *
14	SRVI	Money or value transfer services *
15	R.8	New technologies
16	SRVII	Wire transfers *
		Reliance, Controls and Financial Groups
17	R.9	Reliance on third parties *
18	R.15 & R.22	Internal controls and foreign branches and subsidiaries *
19	R.21	Higher-risk countries *
		Reporting of suspicious transactions
20	R.13 & SRIV	Reporting of suspicious transactions *
21	R.14	Tipping-off and confidentiality
		Designated non-financial Businesses and Professions (DNFBPs)
22	R.12	DNFBPs: Customer due diligence *
23	R.16	DNFBPs: Other measures *

		E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
24	R.33	Transparency and beneficial ownership of legal persons *
25	R.34	Transparency and beneficial ownership of legal arrangements *
		F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
		Regulation and Supervision
26	R.23	Regulation and supervision of financial institutions *
27	R.29	Powers of supervisors
28	R.24	Regulation and supervision of DNFBPs
		Operational and Law Enforcement
29	R.26	Financial intelligence units *
30	R.27	Responsibilities of law enforcement and investigative authorities *
31	R.28	Powers of law enforcement and investigative authorities
32	SRIX	Cash couriers *
		General Requirements
33	R.32	Statistics
34	R.25	Guidance and feedback
		Sanctions
35	R.17	Sanctions
		G – INTERNATIONAL COOPERATION
36	R.35 & SRI	International instruments
37	R.36 & SRV	Mutual legal assistance
38	R.38	Mutual legal assistance: freezing and confiscation *
39	R.39	Extradition
40	R.40	Other forms of international cooperation *

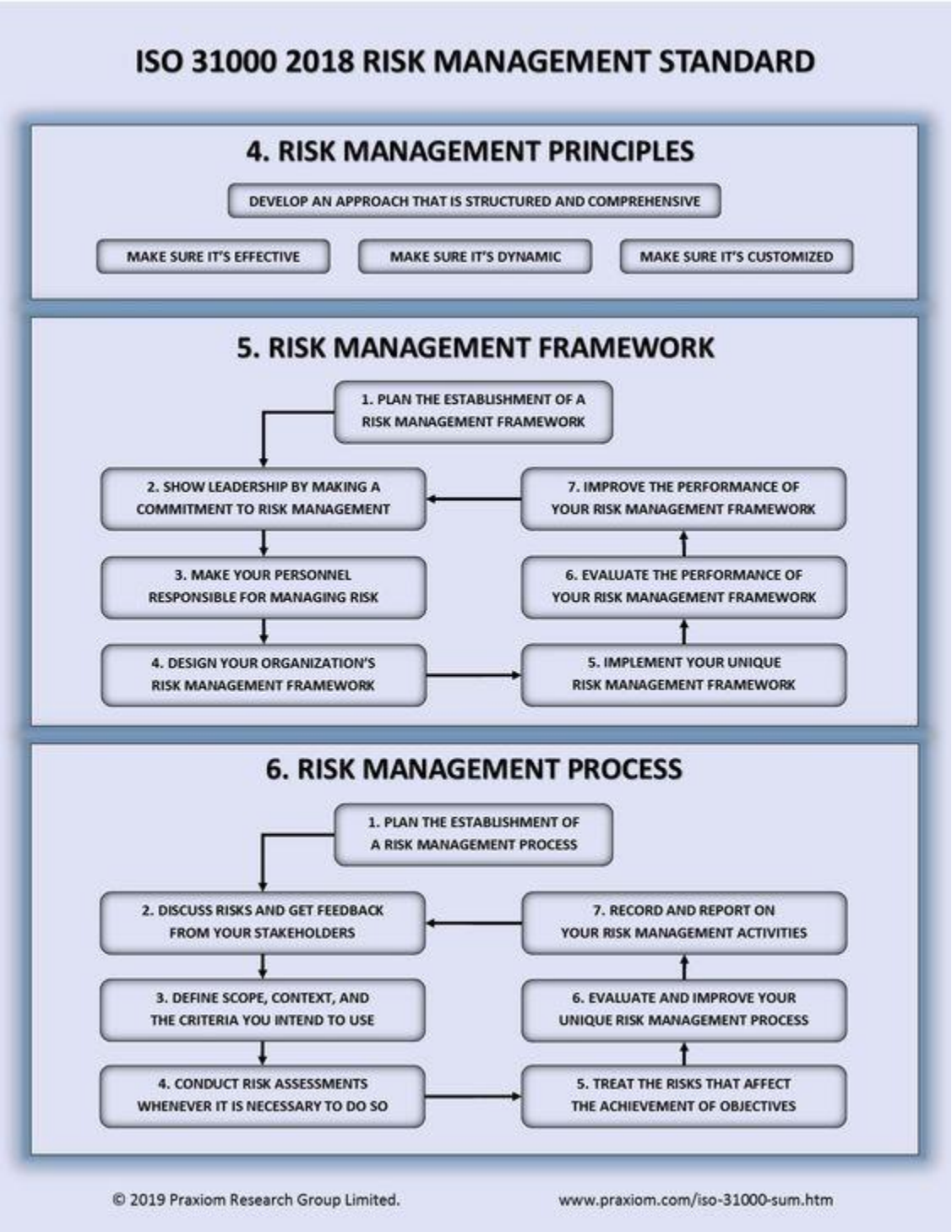
1. The 'old number' column refers to the corresponding 2003 FATF Recommendation.

** Recommendations marked with an asterisk have interpretive notes, which should be read in conjunction with the Recommendation.*

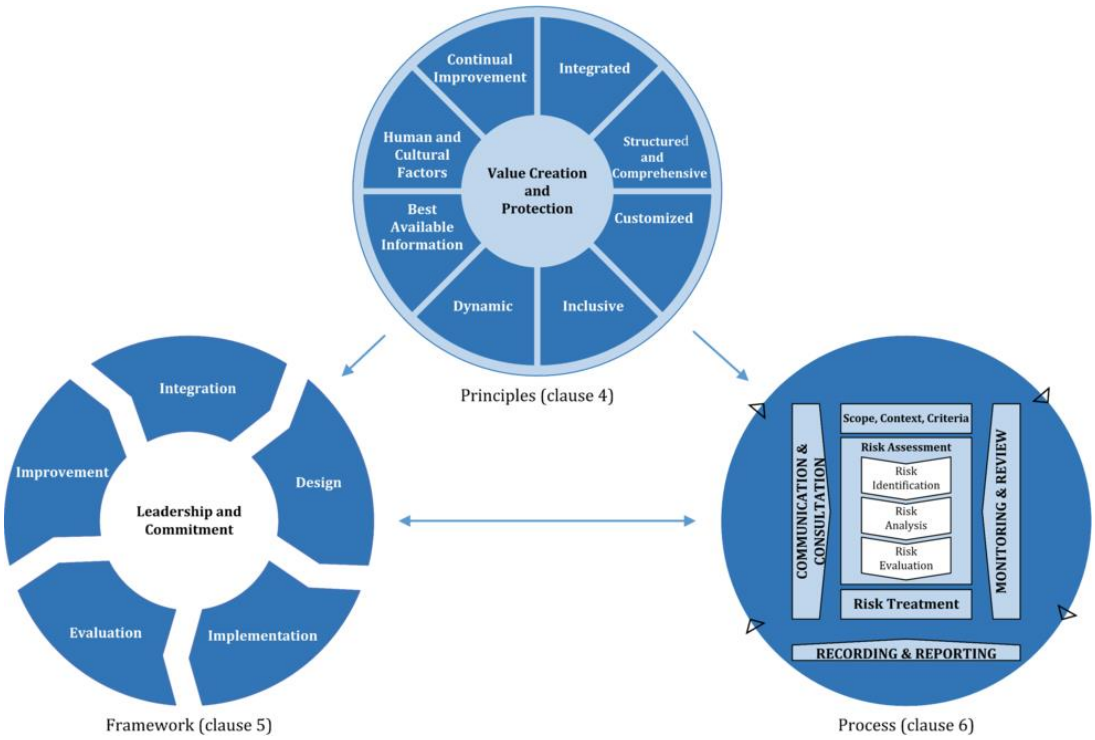
Version as adopted on 15 February 2012.

Source: The Financial Action Task Force (FATF)

Appendix 3: ISO 31000 2018 Risk Management Standard

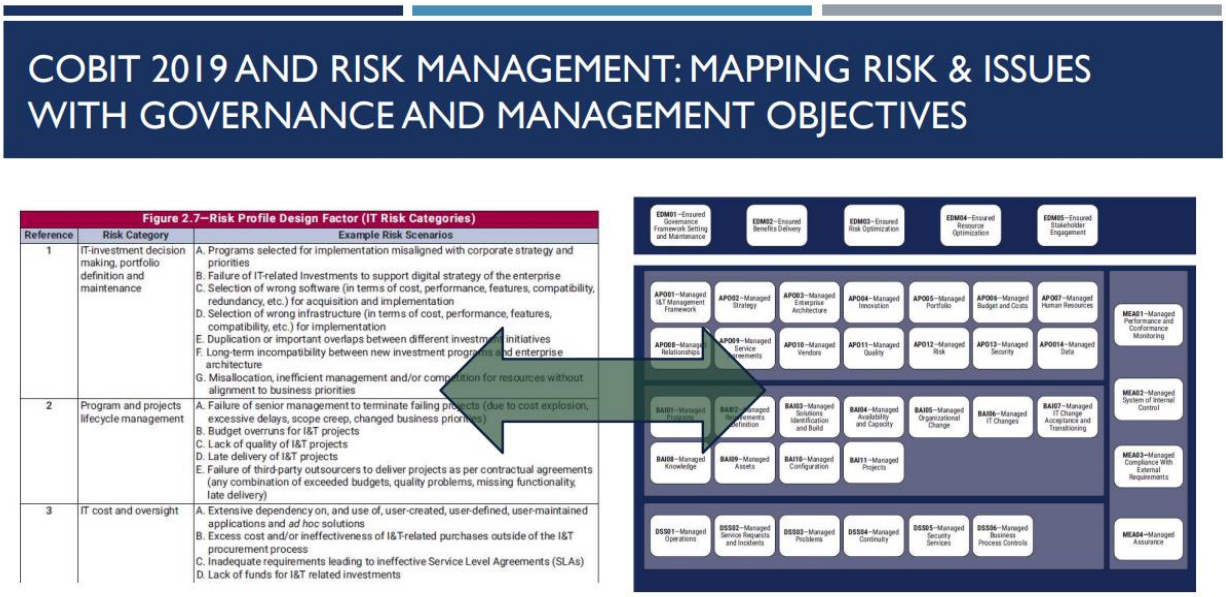


Appendix 4: Depicts Risk Management Principles, Framework, and Process



Sources: ISO 13000 2018 Risk Management Guidelines

Appendix 5: Depicts Mapping Risk Issues with Governance and Management Objectives:



References

ACFE Report to the Nations on Occupational Fraud and Abuse, published by the Association of Certified Fraud Examiners (2018).
http://www.acfe.com/rttn2016.aspx. (Accessed Apr. 6, 2020)

ACFE Report to the Nations on Occupational Fraud and Abuse, published by the Association of Certified Fraud Examiners (2018). http://www.acfe.com/rttn2016.aspx.
(Accessed Apr. 6, 2020)

Ammerman, Darcy, Ricchetti Alex, and Forgione , Pat, Banking Regulation 2019 March 2019. https://mcmillan.ca/Banking-Regulation-2019 (Assessed Apr. 9, 2020)

Anderson, Richard, Frigo, Mark, COSO- Creating and Protecting Value: Understanding and Implementing Enterprise Risk Management January 2020. https://www.coso.org/Documents/COSO-ERM-Creating-and-Protecting-Value.pdf accessed May 18,2020

Anti-money laundering and counter-terrorist financing measures- Canada Mutual Evaluation Report 2016 http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Canada-2016.pdf accessed May 6,2020

Bradley Hope, Drew Hinshaw, and Patricia Kowsmann, "How One Stubborn Banker Exposed a $200 billion Russian Money-Laundering Scandal," *Wall Street Journal,* October 23, 2018, accessed May 6, 2020, at https://www.wsj.com/articles/how-one-stubborn-banker-exposed-a-200-billion-russian-money-laundering-scandal-1540307327.

CA-IFA, CA-EJC Investigative & Forensic Accounting Juricomptabilite: Standard Practices for Investigative and Forensic Accounting Engagements (Nov. 2006)
file:///C:/Users/Kenny/Downloads/00230-EP_Standard_Practices_for_Investigative_and_Forensic_Accounting_Engagements_04_14_2015%20(5).pdf. Accessed May 8, 2020

Characteristics of Forensic Audit and differences in relation to external audit. Predrag Vukadinović*, Goranka Knežević, Vule Mizdraković. Singidunum University, Faculty of Business in Belgrade, 32 Danijelova Street, Belgrade, Serbia. http://portal.finiz.singidunum.ac.rs/Media/files/2015/202-205.pdf (Accessed April 9,2020)

Core principles for effective banking supervision. BIS December 20, 2011 https://www.bis.org/publ/bcbs213.htm. (Assessed Apr. 9, 020)

Corporate Compliance Insight- The Premier Global News Source for Compliance, Ethics, Audit & Risk: The Curious Case of Bias in Risk Assessment by Christoper Magno, Terrance Mccne, and Michael G. Gordon 2019 https://www.corporatecomplianceinsights.com/risk-assessments-cognitive-bias/ (Assessed Apr. 25, 2020).

COSO 2017 Enterprise Risk Management Integrating With Strategy And Performance. https://teolupus.com/teo/en/june-2017-coso-enterprise-risk-management-integrating-with-strategy-and-performance/ (Accessed May 26, 2020)

COSO Enterprise Risk Management- Integrating with Strategy and Performance. https://www.pwc.com/us/en/services/consulting/risk-regulatory/coso-erm-framework.html (Accessed May 18, 2020)

Crumbley Text 5th Edition- The field and practice of forensic accounting: University of Toronto MFAcc IFA 2905 Reading Material 2017

Danske Bank Money Laundering Case Study 2019. https://sites.duke.edu/thefinregblog/2019/09/11/danske-bank-money-laundering-case-study/ (Accessed May 25, 2020)

Danske Bank. 2018. "Findings of the Investigation Relating to Danske Banks' Branch in Estonia," Danske Bank. https://danskebank.com/news-and-insights/news-archive/press-releases/2018/pr19092018 (Accessed Apr. 26, 2020)

Data mining and information sharing: Two essential tools to stop insurance fraud and abuse. By Daniel Tourangeau CPA, CA, CA-IFA, CFF (2017). University of Toronto MFAcc IFA 2905 H Materials

Deloitte Center for Regulatory Strategy: Managing Conduct Risk 2017 https://www2.deloitte.com/global/en/pages/financial-services/articles/managing-conduct-risk.html (Accessed Mar. 25, 2020)

DeRitis, Christian. Managing the Risk Multiverse with Scenarios: How to Be Better Prepared for the Next Pandemic June 8, 2020. https://www.moodysanalytics.com/-/media/article/2020/managing-the-risk-multiverse-with-scenarios.pdf (June 8, 2020)

Economist. 2019. "A Massive Money-Laundering Scandal Stains the Image of Nordic Banks," The Economist, October 17, 2019. https://www.economist.com/finance-and-economics/2019/10/17/a-massive-money-laundering-scandal-stains-the-image-of-nordic-banks accessed April 27,2020

Enterprise Risk Management| Applying enterprise risk management to environmental, social, and performance related risks. October 2018. https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf (Accessed May 18, 2020)

Essential risk management skills that every manager should have- https://www.rapidglobal.com/blog/10-essential-risk-management-skills-that-every-manager-should-have/ (Accessed Feb. 20, 2020)

Forensic Accounting and Investigation: A means of curbing Money Laundering Activities Being a paper delivered by Chief Godwin Emmanuel Oyedokun, at the Nigerian Students' Economic and Finance Summit (NISEF) 2014 of Obafemi Awolowo University: Putting Nigeria on the Pedestal of Sustainable Economic Development; Challenges Strategies and Way Forward. https://docplayer.net/54888318-Forensic-accounting-and-investigation-a-means-of-curbing-money-laundering-activities-oau-nuasa-march-28-2014.html (Accessed Mar. 25, 2020)

Forensic Auditing and Artificial Intelligence Help Detect Fraudulent Activity By Mac Lillard, CPA, CFE, CITP, CISA, PCIP | GRF Audit Supervisor https://www.grfcpa.com/2019/02/forensic-auditing-and-artificial-intelligence-help-detect-fraudulent-activity/ (Assessed Apr. 9, 2020)

From Risk to Opportunity – Accountants Need to Lead Enterprise Risk Management By Stuart Chaplin, Stathis Gould (2019) https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/risk-opportunity-accountants-need (Accessed May 14, 2020)

Global Legal Insights: Canada Banking Regulation (2019) by Pat Forgione, Darcy Ammerman and Alex Ricchetti of McMillan LLp https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/canada Assessed Mar. 16, 2020

Harvard Business Review - Strategic Planning |Managing Risk: A new Framework. https://hbr.org/2012/06/managing-risks-a-new-framework (Accessed May 25, 2020)

International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation of the FATF Recommendations- updated 2019 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (Accessed June 5, 2020)

ISACA: COBIT 2019 and Risk Management https://isaca.nl/wp-content/uploads/Downloads/Risk%20Event/2019/Dirk_Steuperaert_IT_in_Balance_BVBA_Uni_Gent_Uni_Antwerpen_Cobit_2019.pdf (Accessed June 8, 2020)

ISO 31000:2018 Risk management — Guidelines February 2018. https://www.iso.org/standard/65694.html (Assessed Apr. 9, 2020)

Journal of Forensic & Investigative Accounting (JFIA) Vol. 4, Issue 1, 2012 : Teaching Interviewing Techniques to Forensic Accountants Is Critical by Scott F. Porter and D. Larry Crumbley. https://s3.amazonaws.com/web.nacva.com/JFIA/Issues/JFIA-2012-1_5.pdf (Accessed Apr. 24, 2020)

Journal of Sustainable Development in Africa Vol. 10, No.4, 2009: The Effectiveness of Forensic Auditing in Detecting, Investigating, and Preventing Bank Frauds

Mckinsey Working Papers on Risk: The future of a bank risk management Authored by: Phillipp Harle, Andras Havas, Andreas Kremer, Daniel Rona and Hamid Samandari 2016 https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-bank-risk-management Accessed Apr. 13, 2020

Meyer Aaron, Jim Armstrong, and Mark Zelmer, Financial System Review: "An Overview of Risk Management at Canadian Banks" 2012. https://www.bankofcanada.ca/wp-content/uploads/2012/01/fsr-0607-aaron.pdf (Accessed June 1, 2020)

Money Laundering: The Role of a Forensic Accountant as an Expert Witness. https://www.mbamaassociates.com/?q=node/5 (Accessed June 1, 2020)

OSFI E21 Operational Risk Management 2017 https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/e21_gias.aspx Accessed Apr. 13, 2020

Report on the Non-Resident Portfolio at Danske Bank's Estonian branch 2018

Risk Assessment Perspectives for Forensic Accountants and Auditors Based on some International Evidence. Journal of Forensic and Investigative Accounting (JFIA)Vol. 9, Issue 1, 2017 https://abfa.us/wp-content/uploads/2017/01/JFIA-2017-No1-5.pdf (Accessed Mar. 4, 2020)

Risk Management Problems: Risk Management Challenges in the Financial Institutions-Abdulhameed Atif Jastaniyah: American Journal of Engineering Research (AJER) 2017. Vol. 6, Issue 4, pp 34-39. http://www.ajer.org/papers/v6(04)/E06043439.pdf (Accessed Feb. 2,2020)

Stempel, Jonathan, Aubin Dena, Reuters 2019 Wells Fargo officials enter $240 million settlement over bogus accounts. March 1, 2019. https://www.reuters.com/article/us-wells-fargo-settlement-idUSKCN1QI4P3 (Accessed May 25, 2020)

The field and practice of forensic accounting: Crumbley Text 5th Edition- MFAcc Reading Material 2017

The Place of Risk Management in Financial Institutions by George S. Oldfield, Anthony M. Santomero. Financial Institutions Center, The Wharton School University of Pennsylvania
The Role of the SEVESO Directives and the Basel Accords in Enterprise Risk Management- M. Mendes da Cruz(Associate Professor IPL- Instituto Politecnico de Lisboa) and Sonia R. Bentes (Assistant Professor of ISCAL)
http://www.aeca1.org/xviencuentroaeca/cd/90d.pdf (Accessed Mar. 25, 2020)

The Roles of Forensic Accountants In Prevention And Detection Of Money Laundering In Phoenix Activities. https://www.researchgate.net/publication/337016613_The_Roles_Of_Forensic_Accountants_In_Prevention_And_Detection_Of_Money_Laundering_In_Phoenix_Activities (Accessed June 1, 2020)

The story of the whistleblowing, including what was involved and how it was discovered, is told in a fascinating account by Bradley Hope, Drew Hinshaw, and Patricia Kowsmann titled "How One Stubborn Banker Exposed a $200 billion Russian Money-Laundering Scandal" in the *Wall Street Journal* of October 23, 2018. https://www.wsj.com/articles/how-one-stubborn-banker-exposed-a-200-billion-russian-money-laundering-scandal-1540307327.(Accessed Apr. 26, 2020)

The Value of Forensic Accountants in Investigations Global Investigation Review(GIR)- Kelvin Shergold of Grant Thornton UK LLP(Nov. 2018)
https://globalinvestigationsreview.com/insight/the-european-middle-eastern-and-african-investigations-review-2018/1177401/the-value-of-forensic-accountants-in-investigations
(Accessed Feb. 22, 2020)

The Wharton School University of Pennsylvania: The Place of risk management in financial institutions.
https://www.researchgate.net/publication/2598120_The_Place_of_Risk_Management_in_Financial_Institutions (Accessed Feb. 19, 2020

Tranchard, Sandrine, The New ISO 31000 Keeps Risk Management Simple February 21, 2018 https://www.iso.org/news/ref2263.html (Accessed June 10, 2020)

Tursoy, Turgut. Munich Personal RePEc Archive: Risk management process in Banking Industry. MPRA Paper No. 864272018. https://mpra.ub.unimuenchen.de/86427/1/MPRA_paper_86427.pdf (Accessed Jun 6, 2020)

Wells Fargo: Corporate board lessons learned? May 2020. https://ethicalboardroom.com/wells-fargo-corporate-board-lessons-learned/ (Accessed May 25, 2020)